

# COUNTING AND EFFECTIVE RIGIDITY IN ALGEBRA AND GEOMETRY

BENJAMIN LINOWITZ, D. B. MCREYNOLDS, PAUL POLLACK, AND LOLA THOMPSON

**ABSTRACT.** The purpose of this article is to produce effective versions of some rigidity results in algebra and geometry. On the geometric side, we focus on the spectrum of primitive geodesic lengths for arithmetic hyperbolic 2- and 3-manifolds. By work of Reid and Chinburg–Hamilton–Long–Reid, this spectrum determines the commensurability class of the manifold. We establish effective versions of these rigidity results by ensuring that, for two incommensurable arithmetic manifolds of bounded volume, the primitive length sets must disagree for a length that can be bounded as a function of volume. We also prove an effective version of a similar rigidity result recently established by the second author with Reid on a surface analog of the primitive length spectrum for hyperbolic 3-manifolds. These effective results have corresponding algebraic analogs involving maximal subfields and quaternion subalgebras of quaternion algebras. To prove these effective rigidity results, we establish results on the asymptotic behavior of certain algebraic and geometric counting functions which are of independent interest.

## 1. INTRODUCTION

This article provides effective solutions to inverse problems in algebra, geometry, and number theory via asymptotic counting results in algebra and geometry which are of independent interest. In this introduction we lay out our main theorems and provide some context and motivation. We initiate this task by establishing a broad platform for inverse problems that will repeatedly service us throughout the remainder of the article.

**1.1. Inverse problems.** We are given a class of objects  $\text{Obj}$  and an invariant that is associated to each object, say  $\text{Inv}(X)$  for each  $X \in \text{Obj}$ . Rigidity or inverse questions in this general framework take the following form:

**Question.** When  $\text{Inv}(X) = \text{Inv}(Y)$ , are the objects  $X, Y$  the same?

Here, “same” refers to whatever natural sense of equality one has for the given set of objects (or a slightly weaker version). We now provide some basic examples directly relevant to this article. We first consider algebraic and number theoretic problems, finishing with geometric ones.

**1.1.1. Algebraic inverse problems.** Given a degree  $d$  central, simple, division algebra  $D$  over a number field  $k$ , the set of isomorphism classes of maximal subfields of  $D$  is a basic invariant of  $D$  that we denote by  $\text{MF}(D)$ .

**Question 1.** Do there exist non-isomorphic, central, simple, division  $k$ -algebras  $D_1, D_2$  with  $\text{MF}(D_1) = \text{MF}(D_2)$ ?

A well-known consequence of class field theory is that when  $D$  is a quaternion algebra, that is when  $D$  is of degree 2,  $\text{MF}(D) = \text{MF}(D')$  if and only if  $D$  and  $D'$  are isomorphic as  $k$ -algebras. Unfortunately, for

higher degree algebras this rigidity is too much to ask of this invariant since the opposite algebra  $D^{\text{op}}$  always has the same set of maximal subfields as  $D$  (see [17], [37], and [71] for some recent work on this topic). Quaternion algebras are exceptional in this regard as they are always isomorphic to their opposite algebras. Geometrically, these maximal subfields correspond to geodesics or higher dimensional flat submanifolds in the locally symmetric manifolds associated to the algebra  $D$ .

The **Brauer group**  $\text{Br}(k)$  of a number field  $k$  is the set of Morita equivalence classes  $[A]$  of central, simple  $k$ -algebras  $A$ . The group operation is given by the tensor product  $\otimes_k$  with inverses given by  $[A^{\text{op}}]$  via the isomorphism between  $A \otimes_k A^{\text{op}}$  and  $\text{End}_k(A)$ . Each class  $[A]$  has a unique central, simple, division  $k$ -algebra  $D_A$  and so we will occasionally blur the distinction between  $D_A$  and  $[A]$ .

Another invariant for central, simple algebras arises by first taking a finite extensions  $L$  of  $k$ . We then have a natural map

$$\text{Res}_{L/k}: \text{Br}(k) \longrightarrow \text{Br}(L)$$

defined by extending scalars

$$\text{Res}_{L/k}([A_0]) = [A_0 \otimes_k L].$$

Given a class  $[A] \in \text{Br}(L)$ , the set

$$(\text{Res}_{L/k})^{-1}([A])$$

is the set of Morita equivalence classes  $[A_0]$  in  $\text{Br}(k)$  such that  $[A] = [A_0 \otimes_k L]$ . This set is an invariant for the algebras in the class  $[A]$  and serves as a higher dimensional analog of  $\text{MF}(A)$ . On the geometric side, the classes  $[A_0]$  give rise to non-flat, locally symmetric submanifolds of the locally symmetric manifolds associated to  $A$ . Note that a typical Morita class  $[A]$  will not be in the image of the map  $\text{Res}_{L/k}$ .

Now, for an extension  $L_1$  of  $k$  and a central division  $L_1$ -algebra  $A$ , we can ask the following:

**Question 2.** *Does there exist a finite extension  $L_2/k$  and a central division  $L_2$ -algebra  $A'$  such that*

$$(\text{Res}_{L_1/k})^{-1}([A]) = (\text{Res}_{L_2/k})^{-1}([A']).$$

Again, in this generality, we cannot hope to conclude that  $L_1 \cong L_2$  and  $A \cong A'$  (see [69]). However, when  $L_1, L_2$  are quadratic extensions of  $k$  and  $A$  is a quaternion algebra, we do get the coveted conclusion provided  $(\text{Res}_{L_1/k})^{-1}([A])$  is non-empty.

**1.1.2. Geometric inverse problems.** Two basic and related geometric examples arise in spectral geometry. Given a closed, negatively curved, Riemannian manifold  $M$ , we have an analytic invariant given by the **eigenvalue spectrum**  $\mathcal{E}(M)$  of the Laplace–Beltrami operator acting on  $L^2(M)$ . Similarly, we have a geometric invariant given by the **primitive geodesic length spectrum**  $\mathcal{L}_p(M)$  of lengths  $\ell$  of primitive, closed geodesics. Both geometric invariants of  $M$  are multi-sets of the form

$$\mathcal{E}(M), \mathcal{L}_p(M) = \{(\lambda_j, m_{\lambda_j})\}, \{(\ell_j, m_{\ell_j})\} \subset \mathbf{R} \times \mathbf{N}.$$

The positive integers  $m_{\lambda_j}, m_{\ell_j}$  are called the **multiplicities** and give the dimension of the associated  $\lambda_j$ -eigenspace or the number of distinct occurrences of the particular primitive length  $\ell_j$ , respectively. Two relevant and important consequences of a Riemannian manifold being negatively curved are that every free homotopy class of closed loops contains a unique closed geodesic representative and that the multi-set of lengths of primitive closed geodesics is discrete. Discreteness holds for the eigenvalue spectrum as well. Discreteness in this setting means that the sets without multiplicity  $\{\lambda_j\}, \{\ell_j\}$  are discrete and the

multiplicities  $m_{\lambda_j}, m_{\ell_j}$  are finite for all  $j$ . These spectra are closely related (see, for instance, [36]). In the case when  $M$  is hyperbolic and of dimension 2 or 3, these spectra determine one another by Selberg's trace formula (see [14, Chapter 9, Section 5]). The associated inverse problem for these spectra is the following:

**Question 3.** *Do there exist non-isometric Riemannian manifolds  $M_1, M_2$  such that  $\mathcal{L}_p(M_1) = \mathcal{L}_p(M_2)$  (or  $\mathcal{E}(M_1) = \mathcal{E}(M_2)$ )?*

Starting with Vignéras [92] and Sunada [88], there have been many papers that have produced non-isometric hyperbolic manifolds with identical eigenvalue and primitive geodesic length spectra; such manifolds are said to be isospectral or length isospectral (see [46] for a broader, more substantial story on isospectral constructions). As a result, isospectral manifolds need not be isometric. By construction, the constructions of Vignéras and Sunada produce manifolds that are commensurable. Moreover, for arithmetic hyperbolic 2- or 3-manifolds, they must be commensurable. Reid [84] proved that hyperbolic 2-manifolds with identical primitive length spectra are commensurable provided one of the manifolds is arithmetic. Using Selberg's trace formula, Reid also obtained an identical result for eigenvalue spectra. As arithmeticity is a commensurability invariant, the other manifold is also arithmetic. Chinburg–Hamilton–Long–Reid [21] extended Reid's result on primitive geodesics to arithmetic hyperbolic 3-manifolds. Prasad–Rapinchuk [80] also extended Reid's work for many classes of arithmetic, locally symmetric manifolds. Before the work of Prasad–Rapinchuk, it was already known that Reid's rigidity result could not be extended to general locally symmetric manifolds as Lubotzky–Samuels–Vishne [61] constructed many examples of isospectral, incommensurable compact locally symmetric manifolds using a method similar to but more technical than that of Vignéras.

**1.1.3. Effective rigidity.** Returning to our broad view, given a finite approximation of an object  $X$ , one can usually obtain some upper bound on the complexity of  $X$  via the approximation method. In the setting above, the complexity might be the volume of the manifold or the discriminant of the algebra. In either of these cases, once an upper bound on the complexity is provided, the list of objects satisfying the upper bound is finite. Indeed, basic invariants, like volume or discriminant, though crude, reduce the problem of recognizing our object to a finite problem. For instance, by work of Borel [7] and Borel–Prasad [9], there are only finitely many arithmetic manifolds of a bounded volume. These finiteness results in combination with Reid or Chinburg–Hamilton–Long–Reid imply immediately the existence of an, albeit possibly uncomputable, effective result.

One way to make the above rigidity results effective is to give an a priori bound on how far out we must look within the invariant set. In the above cases, we have a natural way of ordering the individual quantities in the invariant set. This ordering can be done numerically with the discriminant, if the invariants are algebraic, or with length/area/volume, if the invariants are geometric. Thus, our task is to provide, as a function of the complexity of our given object, a termination point in the invariant set where we must search to. An effectively computable bound on the termination point is our primary goal and is what effective rigidity means in this article.

**1.2. Main results: Effective rigidity.** We now state our main geometric and algebraic effective rigidity results. We refer the reader to the notation list found at the beginning of Section 2 for any undefined symbols or terms.

1.2.1. *Geodesics.* Our first result is an effective version of Reid [84] and Chinburg–Hamilton–Long–Reid [21].

**Theorem 1.1 (Effective Length Rigidity).** *Let  $M_1, M_2$  be compact arithmetic hyperbolic 2-manifolds (3-manifolds) with volume less than  $V$ . There exist absolute effectively computable constants  $c_1, c_2$  (respectively,  $c_3$ ) such that if the length spectrum of  $M_1$  agrees with the length spectrum of  $M_2$  for all lengths less than  $c_1 e^{c_2 \log(V) V^{130}}$  (respectively,  $c_3 e^{(\log(V) \log(V))}$ ) then  $M_1$  and  $M_2$  are commensurable.*

By work of Margulis [67], the growth rate for the number of primitive geodesics of length at most  $t$  on a closed, negatively curved manifold is asymptotic to  $e^{ht}/ht$ , where  $h$  is the topological entropy of the geodesic flow (the case of hyperbolic surfaces was treated earlier by Huber [49]). In particular, an upper bound for the number of geodesic lengths that might be used in Theorem 1.1 is

$$\frac{e^{hc_3 e^{(\log(V) \log(V))}}}{hc_3 e^{(\log(V) \log(V))}}.$$

Belolipetsky–Gelander–Lubotzky–Shalev [4, Theorem 1.2] proved the growth rate of arithmetic lattices of covolume at most  $V$  is at least  $V^{c_0 V}$  for a constant  $c_0$  and  $V$  sufficiently large. Accordingly, that forces us to sift through a rather large number of distinct lengths produced by each lattice in the copious supply ensured by [4].

It is unclear how to produce a substantial savings with our approach. More likely, a savings could be achieved by judiciously selecting lengths in sympathy with the manifold we want to recognize. However, in terms of the actual implementation of this strategy, one would need considerable knowledge of the other manifolds that we seek to rule out. Such knowledge seems rather expensive in terms of implementation, even relative to our above asking price, as it requires extensive knowledge of what might be viewed as the state space.

The primary idea in our selection process for the geodesic lengths is that the selected geodesic lengths convey distinct information from those previously selected. We optimize by selecting the smallest possible length that is guaranteed to satisfy this distinction condition. In this way, we ensure definite reduction of the state space at each progression. Note that this relatively simple approach gives an upper bound on the number of selected lengths from an upper bound on the cardinality of the initial state space. In particular, we see a direct connection between effective algorithms/rigidity and counting problems. We will return to this connection when we discuss our counting results below.

In Section 7, we construct two infinite sequences of pairwise incommensurable arithmetic hyperbolic 3-manifolds that show that one cannot check a uniformly bounded number of primitive geodesic lengths. By Theorem 1.1, as  $n$  tends to infinity, the volumes of the manifolds will grow. We have not worked out the explicit growth of the volumes of the manifolds as a function of  $n$  but it seems quite likely to be exponential if not super-exponential in our construction. We also have a result, Theorem 4.11, which shows that there can exist infinitely many commensurability classes of arithmetic hyperbolic 2- or 3-manifolds with a prescribed, finite set of geodesic lengths. Recently, Millichap [72, 73] constructed roughly  $(2n)!$  incommensurable hyperbolic 3-manifolds that have the same first  $2n + 1$  (complex) geodesic lengths. Moreover, the manifolds all have the same volume and the volume of these manifolds grows linearly in  $n$ . His examples are non-arithmetic and his methods are geometric/topological. Neither of these constructions produce lower bounds near the upper bound we provide in Theorem 1.1.

1.2.2. *Totally geodesic surfaces.* Our second result is an effective version of [70, Theorem 1.1]. Before stating our result, we require some additional notation.

For a finite volume hyperbolic 3-manifold  $M$ ,  $GS(M)$  will denote the isometry classes of finite volume, properly immersed, totally geodesic surfaces up to free homotopy. It follows from work of Thurston [91, Corollary 8.8.6.] that  $GS(M)$  contains only finitely many Riemann surfaces of a fixed finite topological type.

**Theorem 1.2 (Effective Geometric Rigidity).** *Let  $M_1, M_2$  be arithmetic hyperbolic 3-manifolds with volumes less than  $V$  and  $GS(M_1) \cap GS(M_2) \neq \emptyset$ . Then there exists an absolute, effectively computable constant  $c$  such that if a finite type hyperbolic surface  $X$  lies in  $GS(M_1)$  if and only if it lies in  $GS(M_2)$  whenever the area of  $X$  is less than  $e^{cV}$ , then  $M_1$  and  $M_2$  are commensurable.*

There are infinitely many commensurability classes  $\mathcal{C}$  of arithmetic hyperbolic 3-manifolds such that all representatives  $M$  in  $\mathcal{C}$  have  $GS(M) = \emptyset$  (see [64, Corollary 7] and [22, p. 546]). However, once an arithmetic hyperbolic 3-manifold has one such surface, it is a well-known fact that there are necessarily infinitely many distinct commensurability classes of such surfaces. Below, Theorem 1.11 provides a lower bound for the number of commensurability classes of surfaces up to some volume in these arithmetic hyperbolic 3-manifold and hence implies the infinitude of such surfaces for those manifolds. To the best of our knowledge the lower bound we provide is the first such lower bound.

1.2.3. *Algebraic.* We now turn to algebraic effective rigidity results which, aside from being independently interesting, provide us with tools for proving the above geometric effective rigidity results. Our first result is an effective version of the fact that quaternion algebras over number fields are determined by their maximal subfields.

**Theorem 1.3 (Effective Maximal Subfields Rigidity).** *Let  $k$  be a number field and let  $B, B'$  be quaternion algebras over  $k$  satisfying*

$$|\text{disc}(B)|, |\text{disc}(B')| < x.$$

*If every quadratic field extension  $L/k$  with*

$$|\Delta_{L/k}| < 64^{n_k^3} d_k^{n_k} e^{2n_k \left[ \frac{21x}{\log^3(x)} + x \right]}$$

*embeds into  $B$  if and only if it embeds into  $B'$  then  $B \cong B'$ .*

We further note that in Theorem 1.3, if the quaternion algebras  $B$  and  $B'$  are both unramified at a common real place of  $k$ , then we need only consider quadratic extensions  $L/k$  which are not totally complex.

Our second result is the algebraic counterpart of our effective result, Theorem 1.2, on totally geodesic surfaces.

**Theorem 1.4 (Effective Brauer Rigidity).** *Suppose that  $L_1, L_2$  are quadratic extensions of a number field  $k$  and  $B_1, B_2$  are quaternion algebras over  $L_1, L_2$  such that*

$$\{\mathfrak{p} \in \mathcal{P}_k : \mathfrak{q} \in \text{Ram}_\infty(B_1), \mathfrak{q} \mid \mathfrak{p}\} = \{\mathfrak{p} \in \mathcal{P}_k : \mathfrak{q} \in \text{Ram}_\infty(B_2), \mathfrak{q} \mid \mathfrak{p}\}.$$

*We further insist that there exists  $B_0$  a quaternion algebra over  $k$  such that*

$$\text{Ram}_\infty(B_0) = \{\mathfrak{p} \in \mathcal{P}_k : \mathfrak{q} \in \text{Ram}_\infty(B_1), \mathfrak{q} \mid \mathfrak{p}\}$$

and additionally satisfies

$$B_0 \otimes_k L_1 \cong B_1, \quad B_0 \otimes_k L_2 \cong B_2.$$

If  $B \otimes_k L_1 \cong B_1$  if and only if  $B \otimes_k L_2 \cong B_2$  whenever  $B$  is a quaternion algebra over  $k$  with

$$\text{Ram}_\infty(B) = \{\mathfrak{p} \in \mathcal{P}_k : \mathfrak{q} \in \text{Ram}_\infty(B_1), \mathfrak{q} \mid \mathfrak{p}\}$$

and discriminant that satisfies

$$|\text{disc}(B)| \leq d_\ell^{2C} (2 \log(|\text{disc}(B_1)| |\text{disc}(B_2)|))^4 |\text{disc}(B_1)| |\text{disc}(B_2)|,$$

then  $L_1 \cong L_2$  and  $B_1 \cong B_2$ .

Here  $C$  is the (absolute) constant appearing in the effective Chebotarev density theorem [53]. Theorem 1.4 is stronger than the algebraic result deduced in [70]. Consequently, Theorem 1.4 provides similar geometric spectral rigidity results but for the broader class of manifolds modeled on products of a finite number of hyperbolic 2-spaces and/or a finite number of hyperbolic 3-spaces. Examples of such manifolds are Hilbert modular varieties and quaternionic Shimura modular varieties. Note that the submanifolds in this broader setting are typically higher dimensional totally geodesic submanifolds.

**1.3. Main tools: Counting function and asymptotic behavior.** As we noted above, our method for establishing the above effective rigidity results relies on controlling the asymptotic growth of certain natural counting functions. We now provide motivation for these algebraic counting results.

Understanding the asymptotic behavior of counting functions is central to the field of analytic number theory. Our work falls within the subfield of arithmetic statistics, which centers around counting problems on number fields and elliptic curves with bounded discriminant. The analytic method used in our proofs goes at least back to Harvey Cohn [25], who used a similar approach to count the number of abelian cubic extensions of  $\mathbf{Q}$  with bounded discriminant. Other seminal works in this area include the classical theorem of Davenport and Heilbronn [28], which provides an asymptotic formula for the number of cubic number fields with bounded discriminant, and its various generalizations to certain classes of number fields of higher degree (for an excellent survey of these results we refer the reader to Bhargava's lecture from the 2006 ICM [6]). The general philosophy used in all of this work is to introduce a generating function whose coefficients count the object being studied and then apply a Tauberian theorem to convert information about the analytic behavior of these functions near their singularities into useful information about the counts. Although the results in this subsection are functioning as tools for proving our above stated results, they fall naturally within this larger program of study and thus are of independent interest. Specifically, the technical results that we discuss below all involve counting problems on central division algebras with bounded discriminant.

**1.3.1. Algebraic.** We now turn to the statements of our main algebraic asymptotic results. Let

$$N_{m,n}(x) := \#\{\text{central simple algebras } A/k \text{ of dimension } n^2 \text{ of the form}$$

$$A = M(r, D), \text{ where } \dim(D) = d^2 \text{ for some } d \mid m, \text{ and } |\text{disc}(A)| \leq x\}.$$

With this notation established, we can now state the result.



**Theorem 1.5 (Growth Rate of Division Algebras).** *If  $N(x)$  denotes the number of division algebras of dimension  $n^2$  over  $k$  and  $\ell$  is the smallest prime divisor of  $n$ , then*

$$N(x) = \sum_{m|n} \mu(n/m) N_{m,n}(x).$$

Moreover, there is a constant  $\delta_n > 0$  so that

$$(1) \quad N(x) = (\delta_n + o(1)) x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2},$$

as  $x \rightarrow \infty$ .

The key component of this proof is a classical Tauberian theorem of Delange, which allows us to precisely estimate  $N_{m,n}(x)$  provided that we understand the analytic behavior of its associated Dirichlet series. Our next result provides a count of the number of quadratic extensions that embed in a fixed quaternion algebra over a fixed number field  $k$ .

**Theorem 1.6 (Growth Rate of Algebras with a Specified Subfield).** *Fix a number field  $k$  and a quaternion algebra  $B$  defined over  $k$ . The number of quadratic extensions  $L/k$  which embed into  $B$  and satisfy  $|\Delta_{L/k}| \leq x$  is asymptotic to  $c_{k,B}x$ , as  $x \rightarrow \infty$ , where  $c_{k,B} > 0$ . Moreover, if  $\kappa_k$  is the residue at  $s = 1$  of  $\zeta_k(s)$ ,  $r_2$  is the number of pairs of complex embeddings of  $k$ , and  $r_B$  is the number of places of  $k$  (both finite and infinite) that ramify in  $B$ , then*

$$c_{k,B} \geq \frac{1}{2^{r_B+r_2}} \frac{\kappa_k}{\zeta_k(2)}.$$

The proof of this result stems from a powerful theorem of Wood [95], which allows us to model the splitting of finitely many primes as mutually independent events, over the class of random extensions of  $k$ . Our final technical theorem provides a count of those quaternion algebras over  $k$  with a specified finite collection of maximal subfields. Note that we require some conditions on the collection of subfields as some selections might not have any algebra that contains them as maximal subfields.

**Theorem 1.7 (Growth Rate of Algebras with Specified Subfields).** *Fix a number field  $k$ , and fix quadratic extensions  $L_1, L_2, \dots, L_r$  of  $k$ . Let  $L$  be the compositum of the  $L_i$ , and suppose that  $[L : k] = 2^r$ . The number of quaternion algebras over  $k$  with discriminant having norm less than  $x$  and which admit embeddings of all of the  $L_i$  is*

$$\sim \delta \cdot x^{1/2} / (\log x)^{1-\frac{1}{2^r}},$$

as  $x \rightarrow \infty$ . Here  $\delta$  is a positive constant depending only on the  $L_i$  and  $k$ , given explicitly in the proof.

In this proof, we make use of the well-developed theory of sums of nonnegative multiplicative functions due to Wirsing in order to obtain a precise asymptotic for our counting function. We highlight an explicit value of the constant  $\delta$  in the case where  $r = 1$  below.

*Example 1.* When  $r = 1$ , the expression for  $\delta$  can be put in compact form. We find that the number of quaternion algebras  $B/k$  that admit an embedding of a fixed quadratic extension  $L/k$  is

$$\sim 2^{r'_1 - \frac{1}{2}} \left( \frac{\kappa}{L(1, \chi)} \right)^{1/2} \cdot \prod_{\substack{p \text{ finite} \\ p \text{ not split}}} \left( 1 - \frac{1}{|p|^2} \right)^{1/2} \cdot \prod_{\substack{p \text{ finite} \\ p \text{ ramified}}} \left( 1 + \frac{1}{|p|} \right)^{1/2} \cdot \frac{x^{1/2}}{(\log x)^{1/2}},$$

as  $x \rightarrow \infty$ . Here  $\kappa$  is the residue at  $s = 1$  of  $\zeta_k(s)$ , and  $L(1, \chi)$  is the value at  $s = 1$  of the nontrivial Artin  $L$ -function associated to the extension  $L/k$ .

1.3.2. *Geometric.* The above algebraic counting results have geometric companions. We briefly supply some additional, independent motivation before stating our geometric counting applications.

**Geometric counting problems.** On the geometric side, there have been a number of important results on growth rates of counting functions. Basic problems like counting arithmetic manifolds of a bounded volume modeled on a fixed symmetric space involve two distinct mechanisms for growth: the growth rate coming from a fixed commensurability class and the growth rate of the number of distinct commensurability classes. Several papers have been written on the growth rate of (arithmetic) lattices in a fixed Lie group and also manifolds modeled on a fixed symmetric space; see, for example, [3], [4], [5], [13], [40], [41], [43], [44], [45], [55], [56], and [60]. Several papers have been written on integer counting problems in homogenous spaces, which provide growth rates coming from a fixed finite set of commensurability classes; see, for example, [2], [31], [33], [34], [35], [47], [74], [86].

The problem of counting commensurability classes has been less extensively studied. Belolipetsky [3] counted maximal arithmetic lattices, a problem that resides somewhere between counting subgroups and counting commensurability classes. Recently, Raimbault [81] followed by Gelander–Levit [41] investigated the growth rate for commensurability classes of hyperbolic  $n$ -manifolds without an arithmetic assumption on the manifolds.

Our geometric counting results focus on counting commensurability classes of manifolds with some prescribed features, or counting commensurability classes of geodesics or totally geodesic submanifolds in a fixed manifold. These results complement results obtained from integer counting methods that yield growth rates coming from finite sets of classes. Our methods are general and can be employed in a much wider range of symmetric spaces with a wide range of constraints placed on the commensurability classes than what we presently explore.

**Main geometric counting results.** Our first two results provide upper bounds for the number of commensurability classes of arithmetic hyperbolic 2- or 3-manifolds with a fixed invariant trace field. In the statement of these results, the volume  $V_{\mathcal{C}}$  of a commensurability class  $\mathcal{C}$  is the minimum volume achieved by its members. That this volume is actually achieved in a commensurability class follows from work of Borel [7] for instance; for non-arithmetic manifolds, this follows immediately from work of Margulis [68, Chapter IX].

Our first geometric counting result gives an upper bound for the number of commensurability classes of arithmetic hyperbolic 2-manifolds with invariant trace field  $k$ .

**Corollary 1.8 (Growth Rate of Commensurability Classes: 2-manifolds).** *Let  $k$  be a totally real number field of degree  $n_k$  and let  $N_k(V)$  denote the number of commensurability classes  $\mathcal{C}$  of compact arithmetic hyperbolic surfaces with invariant trace field  $k$  and  $V_{\mathcal{C}} \leq V$ . Then for all sufficiently large  $V$  we have*

$$N_k(V) \ll \frac{\kappa 2^{n_k-1} V^{130}}{\zeta_k(2)},$$

where  $\zeta_k(s)$  is the Dedekind zeta function of  $k$  and  $\kappa$  is the residue of  $\zeta_k(s)$  at  $s = 1$ .

Our second result is the 3-manifold counterpart to our previous result.



**Corollary 1.9 (Growth Rate of Commensurability Classes: 3-manifolds).** *Let  $k$  be a number field of degree  $n_k$  with a unique complex place and let  $N_k(V)$  denote the number of commensurability classes  $\mathcal{C}$  of compact arithmetic hyperbolic 3-manifolds with invariant trace field  $k$  and  $V_{\mathcal{C}} \leq V$ . Then for all sufficiently large  $V$  we have*

$$N_k(V) \ll \frac{\kappa 2^{n_k-3} V^7}{\zeta_k(2)},$$

where  $\zeta_k(s)$  is the Dedekind zeta function of  $k$  and  $\kappa$  is the residue of  $\zeta_k(s)$  at  $s = 1$ .

For non-compact arithmetic 3-manifolds, the commensurability classes of such manifolds are in bijection with the imaginary quadratic number fields.

Our next result provides a lower bound for the number of rationally inequivalent closed geodesics of bounded length. Here, we say a pair of geodesic lengths  $\ell_1, \ell_2$  are **rationally equivalent** if  $\ell_1/\ell_2 \in \mathbf{Q}$  and **rationally inequivalent** otherwise.

**Corollary 1.10 (Growth Rate of Rational Classes of Geodesics).** *Let  $\Gamma$  be an arithmetic Fuchsian group (respectively, Kleinian group) of covolume  $V$  with invariant trace field  $k$  and quaternion algebra  $B$ . For all sufficiently large  $V, x > 0$  the orbifold  $\mathbf{H}^2/\Gamma$  (respectively,  $\mathbf{H}^3/\Gamma$ ) contains at least*

$$\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$$

rationally inequivalent closed geodesics of length at most  $e^{cV} x^{n_k}$  where  $c$  is an absolute, effectively computable constant.

A slightly different form of this inequality is that there are at least

$$\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} e^{-cV/n_k} \right] \ell^{1/n_k}$$

rationally inequivalent closed geodesics of length at most  $\ell$  provided that  $V$  and  $\ell$  are sufficiently large.

Our final geometric counting result provides a lower bound for the growth rate of incommensurable totally geodesic surfaces of bounded area in an arithmetic hyperbolic 3-manifold that contains at least one totally geodesic surface.

**Theorem 1.11 (Growth Rate of Commensurability Classes of Surfaces).** *Let  $M = \mathbf{H}^3/\Gamma$  be an arithmetic hyperbolic 3-manifold of volume  $V$  with invariant quaternion algebra  $B$  and trace field  $k$ . Suppose that  $M$  contains a totally geodesic surface. Then for all sufficiently large  $x$ ,  $M$  contains at least*

$$\left[ c(k) \text{disc}(B)^{1/2} \right] x / \log(x)^{1/2}$$

pairwise incommensurable totally geodesic surfaces with area at most

$$[2\pi^2 e^{cV}] x.$$

Here  $c(k)$  is a constant depending only on  $k$  and  $c$  is an absolute, effectively computable constant.

Again, a slightly different form of this estimate is that there exist at least

$$\frac{[c(k) \text{disc}(B)^{1/2}] \alpha}{2\pi^2 e^{cV} [\log(\alpha) - \log(2\pi^2) - cV]^{1/2}}$$

pairwise incommensurable surfaces of area at most  $\alpha$ .

Theorem 1.11 in tandem with Theorem 1.2 gives an estimate on the number of surfaces needed to distinguish a pair of incommensurable, arithmetic hyperbolic 3-manifolds with a totally geodesic surface. We prove that if an arithmetic hyperbolic 3-manifold contains a totally geodesic surface then in fact it contains a totally geodesic surface with area bounded above by data from the manifold (see Proposition 6.3).

**1.4. Layout.** The layout of the paper is as follows. In Section 2, we introduce some of the basic concepts, terms, and objects for the paper. In Section 3, we prove the main algebraic counting results. In Section 4, we prove the main geometric counting results. In Section 5, we prove the effective results on geodesic lengths while in Section 6 we prove the results involving surfaces, including the asymptotic results on incommensurable, totally geodesic surfaces. In Section 7, we provide some constructions and discussions that test the limits of our effective rigidity results. In Section 8, we briefly discuss the eigenvalue spectrum.

**Acknowledgements.** The authors would like to thank Jayadev Athreya, Richard Canary, Ted Chinburg, Britain Cox, Peter Doyle, Daniel Fiorilli, Tsachik Gelander, Grant Lakeland, Chris Leininger, Jeff Meyer, Nick Miller, Gopal Prasad, Alan Reid, and Matthew Stover for conversations on the material in this article. The first author was partially supported by an NSF RTG grant DMS-1045119 and an NSF Mathematical Sciences Postdoctoral Fellowship. The second author was partially supported by an NSF grant DMS-1105710. The third author was partially supported by an NSF grant DMS-1402268. The fourth author was partially supported by NSF VIGRE grant DMS-0738586 and by an AMS Simons Travel Grant.

## 2. BACKGROUND

We divide our background material into two subsections. The first lays out the algebraic prerequisites for our article, while the second provides the necessary geometric background, used primarily for establishing some standard geometric language.

**Notation.** The following notation is utilized throughout this article.

- $k$  is a number field and  $L/k$  will be an extension.  $\mathcal{O}_k, \mathcal{O}_k^*, \mathcal{O}_k^1$  will denote the ring of integers, the group of units, and the group of norm one elements, respectively.  $\widehat{k}$  will denote the Galois closure of  $k$ .  $k^+$  will denote the maximal, totally real subfield of  $k$ .
- $\mathcal{P}_k$  will denote the set of places/primes of  $k$ . For  $\mathfrak{p} \in \mathcal{P}_k$ , we denote the norm by  $|\mathfrak{p}|$  and the associated valuation by  $|\cdot|_{\mathfrak{p}}$ . For a place  $\mathfrak{P}$  in  $\mathcal{P}_L$  residing over a place  $\mathfrak{p}$  in  $\mathcal{P}_k$ , we denote this by  $\mathfrak{P} | \mathfrak{p}$  or simply  $\mathfrak{P} |_{\mathfrak{p}}$ . Occasionally,  $\mathfrak{P} |_k$  will denote the prime  $\mathfrak{p}$  in  $\mathcal{P}_k$  that  $\mathfrak{P}$  is over.
- $n_k$  will denote the degree of  $k$  over  $\mathbf{Q}$  and  $r_1(k), r_2(k)$  will denote the number of real and complex places, respectively. When the field is understood, we simply write  $r_1, r_2$ .
- $d_k, \text{Reg}_k$  will denote the absolute discriminant and regulator for  $k$ .  $h_k$  will denote the class number of  $k$ .  $\mathfrak{f}_{L/k}$  will denote the conductor.  $\Delta_{L/k}$  will denote the relative discriminant of an extension  $L/k$ .  $\zeta_k(s)$  is the Dedekind  $\zeta$ -function and  $\kappa_k$  will denote the residue of the pole of  $\zeta_k$  at  $s = 1$ .  $J_k$  will denote the idèle group for  $k$ .
- $D$  is a division algebra over  $k$ .
- $A$  is a central simple algebra over  $k$  with group of invertible elements  $A^\times$  and group of norm one elements  $A^1$ .

- $B$  is a quaternion algebra over  $k$ .
- $\text{disc}(A)$  is the discriminant of a central simple  $k$ -algebra.
- $\text{Ram}(A) \subset \mathcal{P}_k$  will denote the set of ramified places for the algebra.  $\text{Ram}_\infty(A)$  will denote the infinite or archimedean places where the algebra is ramified.  $r_A$  will denote the number of infinite places where the algebra is ramified. That is,  $r_A = |\text{Ram}_\infty(A)|$ . We use the same notation in the event that the algebra  $A$  is a division algebra or a quaternion algebra. Finally,  $\text{Ram}_f(A)$  will denote the finite places where  $A$  is ramified. Therefore  $\text{Ram}(A) = \text{Ram}_f(A) \cup \text{Ram}_\infty(A)$ .
- $\text{nr}$  will denote the reduced norm for a central, simple  $k$ -algebra.
- Given a quaternion algebra  $B$ ,  $k_B$  will denote the maximal abelian extension of  $k$  which has 2-elementary Galois group, is unramified outside of the real places in  $\text{Ram}(B)$ , and in which every finite prime of  $\text{Ram}(B)$  splits completely.
- $\mathcal{O}, \mathcal{E}, \mathcal{D}$  will denote  $\mathcal{O}_k$ -orders in a central simple  $k$ -algebra. For each place  $\mathfrak{p} \in \mathcal{P}_k$ , the completion of  $\mathcal{O}$  at  $\mathfrak{p}$  will be denoted by  $\mathcal{O}_{\mathfrak{p}}$ .
- $\mathbf{H}^2, \mathbf{H}^3$  are real hyperbolic 2- and 3-spaces.
- $M$  will denote an arithmetic hyperbolic 2- or 3-manifold and  $\Gamma$  the associated arithmetic lattice in either  $\text{PSL}(2, \mathbf{R})$  or  $\text{PSL}(2, \mathbf{C})$ . That is  $M = \mathbf{H}^2/\Gamma$  or  $\mathbf{H}^3/\Gamma$ . When  $\Gamma = P\Gamma(\mathcal{O}^1)$ , we write  $\Gamma = \Gamma_{\mathcal{O}}$ .
- We refer to lattices in  $\text{PSL}(2, \mathbf{R})$  as Fuchsian and lattices in  $\text{PSL}(2, \mathbf{C})$  as Kleinian.
- $c, C$  and variously decorated versions will denote constants throughout the paper.
- We will make use of several arithmetic functions in Section 3. As usual, let  $\varphi(n)$  denote the Euler totient function, i.e.,  $\varphi(n)$  represents the number of integers  $m$  satisfying  $1 \leq m \leq n$  with  $\gcd(m, n) = 1$ . Moreover, let  $\mu(n)$  denote the Möbius function, i.e., if  $n$  is square-free then  $\mu(n) = (-1)^k$ , where  $k$  is the number of distinct prime factors of  $n$ ; in all other cases,  $\mu(n) = 0$ .
- We will interchangeably use the Landau “Big Oh” notation,  $f = O(g)$ , and the Vinogradov notation,  $f \ll g$ , to indicate that there exists a constant  $C > 0$  such that  $|f| \leq C|g|$ .
- We write  $f \sim g$  if  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$  and we write  $f = o(g)$  if  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0$ .
- Throughout this article,  $\log(x)$  will refer to the natural logarithm function.

**2.1. Algebraic.** We refer the reader to [16], [54], [66], [76], and [85] for complete, general treatments of the broad material in this subsection.

### 2.1.1. Central simple algebras.

One main algebraic requisite for later discussion is the theory of central simple algebras  $A$  over  $k$  and their orders. We briefly recall some standard results. By the Artin–Wedderburn Structure Theorem [76, p. 49], every such  $A$  is isomorphic to a matrix algebra over a division algebra, say  $A = M(r, D)$ . Here  $r$  and  $D$  are uniquely determined. We require the following theorem in this paper.

**Theorem 2.1.** *Let  $k$  be a number field. Let  $S$  be a finite collection of primes of  $k$  consisting of finite primes and real infinite places. Suppose that for each  $\mathfrak{p} \in S$  we are given a reduced fraction  $\frac{a_{\mathfrak{p}}}{m_{\mathfrak{p}}} \in \mathbf{Q}$  such that*

- (i)  $m_{\mathfrak{p}} > 1$  and  $a_{\mathfrak{p}} > 0$ ,
- (ii)  $\frac{a_{\mathfrak{p}}}{m_{\mathfrak{p}}} = \frac{1}{2}$  whenever  $\mathfrak{p}$  is real,
- (iii)

$$\sum_{\mathfrak{p} \in S} \frac{a_{\mathfrak{p}}}{m_{\mathfrak{p}}} \in \mathbf{Z}.$$

There is a unique division algebra  $D/k$  possessing  $S$  as its set of ramified primes and with Hasse invariants  $\frac{a_p}{m_p}$  for  $p \in S$ . Conversely, every division algebra  $D/k$  arises in this way. The dimension of  $D$  is  $n^2$ , where

$$n := \text{lcm}_{p \in S} [m_p],$$

The discriminant of  $D$  is the modulus of  $k$  given by

$$\text{disc}(D) = \prod_{\substack{p \in S \\ p \text{ real}}} p \prod_{\substack{p \in S \\ p \text{ finite}}} p^{n^2(1-\frac{1}{m_p})}.$$

This theorem is a consequence of the Albert–Brauer–Hasse–Noether theorem (see for instance [76, Section 18.4]) and more generally, the short exact sequence of Brauer groups appearing in local class field theory. Moreover, one can show that

$$\begin{aligned} \text{disc}(A) &= \prod_{\substack{p \text{ real} \\ p | \text{disc}(D)}} p \cdot \left( \prod_{\substack{p \text{ finite} \\ p | \text{disc}(D)}} p \right)^{r^2} \\ &= \prod_{\substack{p \in S \\ p \text{ real}}} p \prod_{\substack{p \in S \\ p \text{ finite}}} p^{n^2(1-\frac{1}{m_p})} \end{aligned}$$

when  $A = M(r, D)$ . Thus,

$$(2) \quad |\text{disc}(A)| = |\text{disc}(D)|^{r^2} = \prod_{\substack{p \in S \\ p \text{ finite}}} |p|^{n^2(1-\frac{1}{m_p})}.$$

By Theorem 2.1,  $D$  corresponds to certain Hasse invariants  $a_p/m_p$  for  $p \in \mathcal{P}$ , and the dimension of  $D$  over  $k$  is  $d^2$  for  $d = \text{lcm}_{p \in \mathcal{P}} [m_p]$ . In the future, the Hasse invariants of  $D$  will also be referred to as the **Hasse invariants of  $A$** . If the dimension of  $A$  over  $k$  is  $n^2$ , then

$$r^2 d^2 = n^2.$$

è

**2.1.2. Parametrizing maximal orders.** In what follows below,  $k$  will denote a fixed number field and  $B$  a quaternion algebra defined over  $k$ . The principal purpose of this section is to parameterize, in as effective a manner as possible, the isomorphism classes of maximal orders in  $B$ . Our exposition follows Sections 3 and 4 of [57]. We refer the reader to Reiner [85] for a general treatment on orders.

Let  $J_k$  (respectively  $J_B$ ) denote the idèle group of  $k$  (respectively  $B$ ). In this context, the idèle group  $J_B$  acts on the set of maximal orders of  $B$  as follows. Given  $\tilde{x} \in J_B$  and  $\mathcal{O}$  a maximal order of  $B$  we define  $\tilde{x}\mathcal{O}\tilde{x}^{-1}$  to be the unique maximal order of  $B$  with the property that for every finite prime  $p$  of  $k$ , its completion at  $p$  is equal to  $x_p \mathcal{O}_p x_p^{-1}$  (existence and uniqueness follow from the local-to-global correspondence for orders). With this action we see that the set of maximal orders corresponds to the coset space  $J_B/\mathfrak{N}(\mathcal{O})$ , where

$$\mathfrak{N}(\mathcal{O}) = J_B \cap \prod_p N_{B_p^*}(\mathcal{O}_p)$$

and  $N_{B_p^*}(\mathcal{O}_p)$  is the normalizer in  $B_p^*$  of  $\mathcal{O}_p^*$ . The isomorphism classes of maximal orders of  $B$  (which by the Skolem–Noether theorem [76, p. 230] coincide with conjugacy classes) thus correspond to points in the

double coset space  $B^* \backslash J_B / \mathfrak{N}(\mathcal{O})$ . The reduced norm  $\text{nr}(\cdot)$  induces a bijection [57, Theorem 4.1] between the latter double coset space and

$$k^* \backslash J_k / \text{nr}(\mathfrak{N}(\mathcal{O})) \cong J_k / k^* \text{nr}(\mathfrak{N}(\mathcal{O})).$$

The latter group is finite and, as  $J_k^2 \subset \text{nr}(\mathfrak{N}(\mathcal{O}))$ , is of exponent 2. Hence, there exists an integer  $m \geq 1$  such that the number of isomorphism classes of maximal orders is equal to  $2^m$  and

$$J_k / k^* \text{nr}(\mathfrak{N}(\mathcal{O})) \cong (\mathbf{Z}/2\mathbf{Z})^m.$$

We now parameterize the maximal orders of  $B$ . Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_m$  be a set of primes of  $k$  such that  $B_{\mathfrak{p}_i} \cong \mathbf{M}(2, k_{\mathfrak{p}_i})$  for all  $i$  and such that the cosets of  $J_k / k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$  defined by the elements

$$\{e_{\mathfrak{p}_i} = (1, \dots, 1, \pi_{\mathfrak{p}_i}, 1, \dots)\}_{i=1}^m$$

form a generating set. For each prime  $\mathfrak{p}_i$ , let  $\delta_i = \text{diag}(\pi_{\mathfrak{p}_i}, 1)$  and  $\mathcal{O}'_{\mathfrak{p}_i} = \delta_i \mathcal{O}_{\mathfrak{p}_i} \delta_i^{-1}$ . Given an element  $\gamma = (\gamma_i) \in (\mathbf{Z}/2\mathbf{Z})^m$ , we define a maximal order  $\mathcal{O}^\gamma$  via the local-to-global correspondence:

$$\mathcal{O}_{\mathfrak{p}}^\gamma = \begin{cases} \mathcal{O}_{\mathfrak{p}_i} & \text{if } \mathfrak{p} = \mathfrak{p}_i \text{ and } \gamma_i = 0 \\ \mathcal{O}'_{\mathfrak{p}_i} & \text{if } \mathfrak{p} = \mathfrak{p}_i \text{ and } \gamma_i = 1 \\ \mathcal{O}_{\mathfrak{p}} & \text{otherwise.} \end{cases}$$

Proposition 4.1 of [57] shows that every maximal order of  $B$  is conjugate to one of the orders defined above. Henceforth we will refer to this as a **parameterization of the maximal orders of  $B$  relative to  $\mathcal{O}$** .

Let  $L/k$  be a quadratic field extension and  $k_B$  be the class field corresponding to  $J_k / k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$  by class field theory. Alternatively,  $k_B$  can be characterized as the maximal abelian extension of  $k$  which has 2–elementary Galois group, is unramified outside of the real places in  $\text{Ram}(B)$  and in which every finite prime of  $\text{Ram}(B)$  splits completely. The proof of the following lemma can be found in [57, Lemma 3.7]:

**Lemma 2.2.** *Let the notation be as above.*

- (i) *If  $L \not\subset k_B$  then we may take all of the  $\mathfrak{p}_i$  above to split in  $L/k$ .*
- (ii) *If  $L \subset k_B$  then let  $\mathfrak{q}$  be any prime of  $k$  which is inert in  $L/k$ . Then we may take  $\mathfrak{p}_1 = \mathfrak{q}$  and choose  $\mathfrak{p}_2, \dots, \mathfrak{p}_m$  so that they all split in  $L/k$ .*

We conclude this section with a technical result which we will utilize in the proof of Theorem 1.1.

**Proposition 2.3.** *Let  $\mathcal{E}, \mathcal{D}$  be maximal orders of  $B$  and suppose that  $u \in \mathcal{E}^1$  with  $u \notin k$ . Then there exists an absolute constant  $C_1 > 0$  and a positive integer  $n \leq d_L^{C_1}$  such that  $\mathcal{D}$  admits an embedding of  $\mathcal{O}_k[u^n]$ .*

In the proof of Proposition 2.3, we require the following lemma, which is an immediate consequence of the effective Chebotarev density theorem [53].

**Lemma 2.4.** *Let  $k$  be a number field and let  $L/k$  be a quadratic field extension. Let  $d_L$  denote the absolute discriminant of  $L$ . Then there exists an absolute, effectively computable constant  $C_1$  such that there exists a prime of  $k$  which is inert in  $L/k$  and has norm less than  $d_L^{C_1}$ .*

*Proof of Proposition 2.3.* We begin by setting  $L = k(u)$ . If  $L \not\subset k_B$ , then the selectivity theorem of Chinburg and Friedman [19] (see also [57]) shows that  $\mathcal{D}$  admits an embedding of  $\mathcal{O}_k[u]$ , hence we may take  $n = 1$ .

Suppose now that  $L \subset k_B$  and let  $\mathfrak{q}$  be a prime of  $k$  of smallest norm which is inert in  $L/k$ . Applying Lemma 2.2, we may choose a set of representatives  $\{e_{\mathfrak{p}_i}\}$  of  $J_k/k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$  where  $\mathfrak{p}_1 = \mathfrak{q}$  and  $\mathfrak{p}_2, \dots, \mathfrak{p}_m$  split in  $L/k$ . We claim that  $\mathfrak{q}$  does not ramify in  $B$ . Indeed, suppose that  $\mathfrak{q}$  ramified in  $B$ . By our characterization of  $k_B$ , it would follow that  $\mathfrak{q}$  would split completely in  $k_B$  and hence in  $L$  as  $L \subset k_B$ . However, this observation contradicts the fact that  $\mathfrak{q}$  is inert in  $L/k$ , proving our claim.

For each  $i = 2, \dots, m$ , we have an  $k_{\mathfrak{p}_i}$ -isomorphism  $f_{\mathfrak{p}_i}: B_{\mathfrak{p}_i} \rightarrow M(2, k_{\mathfrak{p}_i})$  such that

$$f_{\mathfrak{p}_i}(L) \subset \begin{pmatrix} k_{\mathfrak{p}_i} & 0 \\ 0 & k_{\mathfrak{p}_i} \end{pmatrix}.$$

Consequently,

$$f_{\mathfrak{p}_i}(\mathcal{O}_L) \subset \begin{pmatrix} \mathcal{O}_{k_{\mathfrak{p}_i}} & 0 \\ 0 & \mathcal{O}_{k_{\mathfrak{p}_i}} \end{pmatrix},$$

and so  $\mathcal{O}_k[u]$  is contained in two adjacent vertices in the tree of maximal orders of  $M(2, k_{\mathfrak{p}_i})$ . Upon conjugating  $\mathcal{E}$  if necessary, we may assume that  $\{\mathcal{E}^\gamma\}$  is a parameterization of the maximal orders of  $B$  relative to  $\mathcal{E}$ . Additionally, we have  $u \in \mathcal{E}_{\mathfrak{p}_i}^\gamma$  for all  $\gamma$  and  $i = 2, \dots, m$ .

By construction  $\mathcal{E}_{\mathfrak{q}}$  and  $\mathcal{E}'_{\mathfrak{q}}$  are adjacent in the tree of maximal orders of  $M(2, k_{\mathfrak{q}})$ . Thus (see [65, pp. 340])

$$[\mathcal{E}_{\mathfrak{q}}^1 : \mathcal{E}'_{\mathfrak{q}} \cap \mathcal{E}_{\mathfrak{q}}^1] = |\mathfrak{q}|(|\mathfrak{q}| + 1).$$

Setting  $n = |\mathfrak{q}|(|\mathfrak{q}| + 1)$ , we have shown that  $u^n \in \mathcal{E}_{\mathfrak{p}_i}^\gamma$  for all  $\gamma$  and  $1 \leq i \leq m$ . Since  $\mathcal{E}_{\mathfrak{p}}^\gamma = \mathcal{E}_{\mathfrak{p}}$  for all primes  $\mathfrak{p}$  of  $k$  outside of  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$ , we can safely conclude that  $u^n \in \mathcal{E}^\gamma$  for all  $\gamma$ . As every maximal order of  $B$  is isomorphic, hence conjugate, to one of the  $\mathcal{E}^\gamma$ , the proposition is now seen to follow from Lemma 2.4.  $\square$

**2.2. Geometric.** We provide some basic concepts and results in hyperbolic geometry that we will employ later. We refer the reader to Maclachlan–Reid [65] for a thorough treatment of this material.

**2.2.1. Hyperbolic geometry.** Hyperbolic  $n$ -space  $\mathbf{H}^n$  is the real rank one symmetric space associated to the real simple Lie group  $\text{SO}(n, 1)$ . In the case of  $n = 2, 3$ , thanks to exceptional isomorphisms, we can identify the group of orientation preserving isometries of  $\mathbf{H}^2, \mathbf{H}^3$  with  $\text{PSL}(2, \mathbf{R}), \text{PSL}(2, \mathbf{C})$ , respectively. We can view  $\mathbf{H}^2, \mathbf{H}^3$  as the symmetric spaces

$$\mathbf{H}^2 = \text{PSL}(2, \mathbf{R})/\text{SO}(2), \quad \mathbf{H}^3 = \text{PSL}(2, \mathbf{C})/\text{SU}(2).$$

Isometries of  $\mathbf{H}^2, \mathbf{H}^3$  split into three classes depending on the trace of the element. **Elliptic** isometries  $\gamma$  satisfy  $|\text{Tr}(\gamma)| < 2$ , **parabolic** isometries satisfy  $|\text{Tr}(\gamma)| = 2$ , and **hyperbolic** (loxodromic) isometries satisfy  $|\text{Tr}(\gamma)| > 2$ . Note that some authors, for hyperbolic isometries use hyperbolic when the eigenvalues are real with the same trace condition and loxodromic to cover the general case. We will simply refer to hyperbolic isometries as the general case, that is, when  $|\text{Tr}(\gamma)| > 2$  but with no assumption that the eigenvalues are real.



**2.2.2. Hyperbolic manifolds and orbifolds.** To form hyperbolic 2– and 3–manifolds, one takes quotients of  $\mathbf{H}^2, \mathbf{H}^3$  by discrete, torsion-free subgroups of  $\mathrm{PSL}(2, \mathbf{R}), \mathrm{PSL}(2, \mathbf{C})$ . Both  $\mathrm{PSL}(2, \mathbf{R})$  and  $\mathrm{PSL}(2, \mathbf{C})$  are naturally endowed with a topology coming from their Lie group structure. By a **discrete subgroup**  $\Gamma$  of  $\mathrm{PSL}(2, \mathbf{R}), \mathrm{PSL}(2, \mathbf{C})$ , we mean a subgroup that is discrete in the Lie or analytic topology. If  $\Gamma$  has no non-trivial elements of finite order, we say that  $\Gamma$  is **torsion-free**. Finally, equipping  $\mathrm{PSL}(2, \mathbf{R})$  or  $\mathrm{PSL}(2, \mathbf{C})$  with a bi-invariant Haar measure  $m$ , we say that  $\Gamma$  is a **lattice** if  $\Gamma$  is discrete and  $m(\mathbf{H}^2/\Gamma)$  or  $m(\mathbf{H}^3/\Gamma)$  is finite. The resulting quotient space is a complete, finite volume hyperbolic orbifold of dimension 2 or 3. In the event  $\Gamma$  is torsion-free, the resulting quotient space will be a complete, finite volume hyperbolic 2– or 3–manifold. Finally, if the quotient space is compact, we say that  $\Gamma$  is a **cocompact lattice**. The quotient space will then be a closed (compact and without boundary) hyperbolic 2– or 3–orbifold. All elements of finite order are necessarily elliptic. In addition, if  $\Gamma$  is a lattice, then  $\Gamma$  will be cocompact precisely when  $\Gamma$  has no non-trivial parabolic elements. In the setting of arithmetic lattices, which we will introduce shortly, this is a consequence of Mahler’s compactness criterion (see [82]) or the more general Godement compactness criterion (see [42]). Finally, we say two groups  $\Gamma_1, \Gamma_2$  in  $\mathrm{PSL}(2, \mathbf{R}), \mathrm{PSL}(2, \mathbf{C})$  are **commensurable in the wide sense** if there exists  $A \in \mathrm{PSL}(2, \mathbf{R}), \mathrm{PSL}(2, \mathbf{C})$  such that  $\Gamma_1 \cap A^{-1}\Gamma_2A$  is a finite index subgroup of both  $\Gamma_1$  and  $A^{-1}\Gamma_2A$ . This condition is equivalent to the associated orbifolds being commensurable in the Riemannian sense. Namely, the two orbifolds share a common, finite Riemannian cover.

Given a lattice  $\Gamma$  and associated quotient  $M = \mathbf{H}^2/\Gamma, \mathbf{H}^3/\Gamma$ , the orbifold fundamental group of  $M$  will be  $\Gamma$ . When  $\Gamma$  is torsion-free, the orbifold fundamental group will simply be the fundamental group. For a complete, finite volume hyperbolic 2– or 3–orbifold, the **rank** of the orbifold fundamental group will be the minimal number of generators. These groups are known to be finitely presented and hence finitely generated.

**2.2.3. Arithmetic hyperbolic manifolds.** Arithmetic lattices in semisimple Lie groups are a specific type of lattice that arises from algebraic constructions. We will not provide a general definition here but instead give the classification of arithmetic lattices in  $\mathrm{PSL}(2, \mathbf{R}), \mathrm{PSL}(2, \mathbf{C})$ . The classification in full generality was done by Weil and Tits (see [90]) and an overview can be found in [78, p. 78–92]. Borel gave a classification and volume formula for arithmetic lattices in  $\mathrm{PSL}(2, \mathbf{R}), \mathrm{PSL}(2, \mathbf{C})$  in [7]. This classification can also be found in the book of Maclachlan–Reid [65, Chapter 8]. For completeness, we provide a brief overview in this subsection.

Let  $k$  be a totally real field  $k/\mathbf{Q}$  with real places  $\mathfrak{p}_1, \dots, \mathfrak{p}_{r_1}$ . Fix a real place of  $k$  which, reordering if necessary, we denote by  $\mathfrak{p}_1$ . We may select a quaternion algebra  $B$  over  $k$  with the property that  $\mathfrak{p}_j \in \mathrm{Ram}(B)$  if and only if  $j > 1$ . In particular,  $B_{\mathfrak{p}_1} \cong \mathrm{M}(2, \mathbf{R})$  and  $B_{\mathfrak{p}_j} \cong \mathbb{H}$  for  $j > 1$ , where  $\mathbb{H}$  is the quaternions over  $\mathbf{R}$ . Under the first isomorphism, the group of norm one elements  $B^1$  maps into  $\mathrm{SL}(2, \mathbf{R})$ . Selecting an order  $\mathcal{O}$  in  $B$ , the image of  $\mathcal{O}^1$  in  $\mathrm{SL}(2, \mathbf{R})$  is a lattice by work of Borel and Harish-Chandra [8]. The projection to  $\mathrm{PSL}(2, \mathbf{R})$  will also be a lattice and we denote the image by  $P\mathcal{O}^1$ . We say  $\Gamma$  is an **arithmetic lattice** in  $\mathrm{PSL}(2, \mathbf{R})$  if  $\Gamma$  is commensurable in the wide sense with  $P\mathcal{O}^1$  for some totally real number field  $k$ ,  $k$ –quaternion algebra  $B$ , and maximal order  $\mathcal{O}$ .

The construction of arithmetic lattices in  $\mathrm{PSL}(2, \mathbf{C})$  is quite similar. We start with a number field  $k$  with exactly one complex place  $\mathfrak{p}_1$  and real places  $\mathfrak{p}_2, \dots, \mathfrak{p}_{r_1+1}$ . We select a  $k$ –quaternion algebra  $B$  such that  $\mathfrak{p}_j \in \mathrm{Ram}(B)$  if and only if  $j > 1$ . Under the isomorphism  $B_{\mathfrak{p}_1} \cong \mathrm{M}(2, \mathbf{C})$ , the group of norm one elements  $\mathcal{O}^1$  of a maximal order  $\mathcal{O}$  of  $B$  will be an arithmetic lattice in  $\mathrm{SL}(2, \mathbf{C})$  by work of Borel and Harish-Chandra [8]. Projecting onto  $\mathrm{PSL}(2, \mathbf{C})$ , the image  $P\mathcal{O}^1$  is a lattice in  $\mathrm{PSL}(2, \mathbf{C})$ . As before, any lattice commensurable in the wide sense with a lattice of the form  $P\mathcal{O}^1$  will be called an **arithmetic lattice** in  $\mathrm{PSL}(2, \mathbf{C})$ .

In the construction above, we mention a few facts that we will need in the sequel. First, if  $k \neq \mathbf{Q}$ , then  $P\mathcal{O}^1$  will be a cocompact lattice in  $\mathrm{PSL}(2, \mathbf{R})$  since  $B$  is a division algebra. Similarly, if  $k$  is not an imaginary quadratic extension,  $P\mathcal{O}^1$  will be a cocompact lattice in  $\mathrm{PSL}(2, \mathbf{C})$ . In fact, as long as  $B$  is a division algebra,  $P\mathcal{O}^1$  will be a cocompact lattice.

**Remark.** We will often blur the distinction between  $\mathcal{O}^1$  and  $P\mathcal{O}^1$ . In addition, the isomorphism  $B_{\mathfrak{p}_1}$  with  $\mathrm{M}(2, \mathbf{R})$  or  $\mathrm{M}(2, \mathbf{C})$  induces an injection  $\rho: B \rightarrow \mathrm{M}(2, \mathbf{R})$  or  $\mathrm{M}(2, \mathbf{C})$ . We will write  $\Gamma_{\mathcal{O}}$  for  $P\rho(\mathcal{O}^1)$  and say that an arithmetic lattice  $\Gamma$  is **derived from a quaternion algebra** if  $\Gamma < \Gamma_{\mathcal{O}}$  for a maximal order  $\mathcal{O}$ .

Given two arithmetic lattices  $\Gamma_1, \Gamma_2$  arising from  $(k_j, B_j)$ ,  $\Gamma_1, \Gamma_2$  will be commensurable in the wide sense if and only if  $k_1 \cong k_2$  and  $B_1 \cong B_2$  (see [65, Theorem 8.4.1]). We will make repeated use of this fact throughout the remainder of this article. For future reference, we give a formal statement of this result now.

**Theorem 2.5.** *Let  $\Gamma_1, \Gamma_2$  be arithmetic lattices in either  $\mathrm{PSL}(2, \mathbf{R})$  or  $\mathrm{PSL}(2, \mathbf{C})$  with arithmetic data  $(k_1, B_1), (k_2, B_2)$ , respectively. Then  $\Gamma_1, \Gamma_2$  are commensurable in the wide sense if and only if  $k_1 \cong k_2$  and  $B_1 \cong B_2$  as  $k$ -algebras where  $k = k_1 = k_2$ .*

This result was first proven by Takeuchi [89] for arithmetic Fuchsian groups and later extended to the Kleinian case by Macbeath [63] and Reid [83].

Finally, we say that  $M$  is an **arithmetic hyperbolic 2– or 3–orbifold** if the orbifold fundamental group of  $M$  is an arithmetic lattice in  $\mathrm{PSL}(2, \mathbf{R}), \mathrm{PSL}(2, \mathbf{C})$ , respectively. We will make reference to the data  $(k, B)$  given in the construction of the lattice  $P\mathcal{O}^1$  as basic invariants of  $M$  since the pair uniquely determines, amongst all arithmetic manifolds, the commensurable class of  $M$ .

The data  $(k, B)$  of an arithmetic hyperbolic 2– or 3–orbifold can be introduced in a different manner in which they are called the **invariant trace field** and **invariant quaternion algebra**. The reader interested in this alternative approach is referred to [65]. We will use that language here as it is both concise and standard. We will sometimes refer to arithmetic lattices in  $\mathrm{PSL}(2, \mathbf{R})$  as **arithmetic Fuchsian groups** and arithmetic lattices in  $\mathrm{PSL}(2, \mathbf{C})$  as **arithmetic Kleinian groups**.

**2.2.4. Geodesics, hyperbolic elements, traces, and quadratic subfields.** Let  $M$  be an arithmetic hyperbolic 2– or 3–orbifold arising from  $(k, B)$  with orbifold fundamental group  $\Gamma < \mathrm{PSL}(2, \mathbf{R})$  or  $\mathrm{PSL}(2, \mathbf{C})$ . The closed geodesics

$$c_{\gamma}: S^1 \longrightarrow M$$

on  $M$  are in bijection with the  $\Gamma$ -conjugacy classes  $[\gamma]_{\Gamma}$  of hyperbolic elements  $\gamma$  in  $\Gamma$ . The roots of the characteristic polynomial  $p_{\gamma}(t)$  are given by the eigenvalues of  $\gamma$  and the associated geodesic length  $\ell(c_{\gamma})$  is given by

$$(3) \quad \cosh\left(\frac{\ell(c_{\gamma})}{2}\right) = \pm \frac{\mathrm{Tr}(\gamma)}{2}.$$

We denote by  $\lambda_{\gamma}$  the unique eigenvalue of  $\gamma$  with  $|\lambda_{\gamma}| > 1$ .

Each closed geodesic  $c_{\gamma}$  determines a maximal subfield  $k_{\gamma}$  of the quaternion algebra  $B$ . Specifically,  $k_{\gamma} = k(\lambda_{\gamma})$ . As  $\Gamma$  is arithmetic,  $\lambda_{\gamma}$  is in  $\mathcal{O}_{k_{\gamma}}^1$ . We call  $k_{\gamma}$  the **associated field** for the hyperbolic element  $\gamma$  or the closed geodesic  $c_{\gamma}$ . We will occasionally abuse notation and write  $\ell(\gamma)$  to denote the length of the associated closed geodesic  $c_{\gamma}$ .

**2.2.5. Volumes.** In this short subsection, we state an inequality between the rank of the fundamental group  $\pi_1(M)$  of a finite volume, complete hyperbolic 3-manifold  $M$  and the volume of the manifold  $M$ . The specific result can be found in the paper of Gelander [38, Theorem 1.7] (see also Gelander [39, Theorem 1.1] and Belolipetsky–Gelander–Lubotzky–Shalev [4, Theorem 1.5]).

**Theorem 2.6** (Gelander). *There exists a constant  $C$  such that if  $M$  is a complete, finite volume hyperbolic 3-manifold of volume  $V$  and rank  $r$  fundamental group, then  $r \leq CV$ .*

Gelander [38] also controls the number of relations and the lengths of the relations. The later works [39] and [4] prove more general results.

**2.2.6. Totally geodesic surfaces.** In this subsection, we give a necessary and sufficient condition for an arithmetic hyperbolic 3-orbifold to possess a totally geodesic surface. Before stating the result, we mention a slightly simpler description of when this occurs. As described above, associated to an arithmetic hyperbolic 3-orbifold is a pair  $(L, B)$ , where  $L$  is a number field with exactly one complex place and  $B$  is an  $L$ -quaternion algebra that is ramified at all of the real places. If there exists a totally real subfield  $k \subset L$  with  $L/k$  quadratic and a  $k$ -quaternion algebra  $B_0$  such that  $B_0 \otimes_k L \cong B$ , then the pair  $(k, B_0)$  will be data for a commensurability class of arithmetic hyperbolic 2-orbifolds provided that  $B_0$  is unramified at the real place  $\mathfrak{P}$  under the complex place  $\mathfrak{P}$  of  $K$ .

The following result can be found in [65, Theorem 9.5.5]. In the statement below,  $\text{Ram}_f(B)$  will denote the finite primes in  $\text{Ram}(B)$ .

**Theorem 2.7.** *Let  $\Gamma$  be an arithmetic lattice in  $\text{PSL}(2, \mathbb{C})$  with arithmetic data  $(L, B)$  and suppose that  $k$  is a totally real subfield of  $L$  with  $[L : k] = 2$ . Suppose  $B_0$  is a quaternion algebra over  $k$  ramified at all real places of  $k$  except at the place under the complex place of  $L$ . Then  $B \cong B_0 \otimes_k L$  if and only if  $\text{Ram}_f(B)$  consists of  $2r$  places (possibly zero)  $\{\mathfrak{P}_{i,j}\}$  where  $j$  ranges over  $\{1, \dots, r\}$  and  $i$  ranges over  $\{1, 2\}$  and satisfy*

$$\mathfrak{P}_{1,j} \cap \mathcal{O}_k = \mathfrak{P}_{2,i} \cap \mathcal{O}_k = \mathfrak{p}_i,$$

*$\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \subset \text{Ram}_f(B_0)$  with  $\text{Ram}_f(B_0) \setminus \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$  consisting of primes in  $\mathcal{O}_k$  which are inert or ramified in  $L/k$ .*

Note that when  $(L, B)$  satisfy the above conditions, there are infinitely many algebras  $B_0/k$  such that  $B \cong B_0 \otimes_k L$ . In particular, any associated arithmetic hyperbolic 3-orbifold will contain infinitely many primitive, totally geodesic, incommensurable surfaces. Note here that a totally geodesic surface is primitive if the immersion is generically one-to-one or equivalently, the immersion does not factor through a proper cover.

### 3. MAIN TOOLS: ALGEBRAIC COUNTING RESULTS

We now begin our first main section, where we will establish our algebraic counting results. For the reader interested only in the applications of these results to the rigidity theorems stated in the introduction, the reader can start at Section 5 and refer back to the results from Sections 3 and 4.

**3.1. Theorem 1.5: Counting algebras of bounded discriminant.** Fix a number field  $k$  and fix a positive integer  $n$ . In this section, we estimate the number of division algebras  $D/k$  of dimension  $n^2$  whose discriminant lies below a large bound  $x$ . Our main weapon is the following Tauberian theorem of Delange [29] and [30].

**Theorem 3.1** (Delange). *Let*

$$G(s) = \sum_{N=1}^{\infty} a_N N^{-s}$$

*be a Dirichlet series satisfying the following conditions for certain real numbers  $\rho > 0$  and  $\beta > 0$ :*

- (i) *each  $a_N \geq 0$ ,*
- (ii)  *$G(s)$  converges for  $\Re(s) > \rho$ ,*
- (iii)  *$G(s)$  can be continued to an analytic function in the closed half-plane  $\Re(s) \geq \rho$ , except possibly for a singularity at  $s = \rho$  itself,*
- (iv) *there is an open neighborhood of  $\rho$ , and functions  $A(s)$  and  $B(s)$  analytic at  $s = \rho$ , with*

$$G(s) = \frac{A(s)}{(s - \rho)^\beta} + B(s)$$

*at every point in  $s$  in this neighborhood having  $\Re(s) > \rho$ .*

*Then as  $x \rightarrow \infty$ ,*

$$\sum_{N \leq x} a_N = \left( \frac{A(\rho)}{\rho \Gamma(\beta)} + o(1) \right) x^\rho (\log x)^{\beta-1}.$$

**Remark.** We allow the possibility that  $A(\rho) = 0$ , in which case the conclusion of Theorem 3.1 is that

$$\sum_{N \leq x} a_N = o(x^\rho (\log x)^{\beta-1}),$$

as  $x \rightarrow \infty$ . While Delange's theorem is usually stated with the restriction that  $A(\rho) \neq 0$ , the cases when  $A(\rho) = 0$  follow with no extra difficulty. For instance, suppose that  $\rho$  is the reciprocal of a positive integer, a condition that holds in all of our applications. If  $A(\rho) = 0$ , we can apply the restricted theorem first to  $G(s) + \zeta(s/\rho)^\beta$ , then to  $\zeta(s/\rho)^\beta$ , and then subtract the results to get the assertion we want. If  $\rho$  is not the reciprocal of a positive integer, then  $\zeta(s/\rho)$  need not be a Dirichlet series itself. However, this argument still works, provided we take as our starting point Delange's original Tauberian theorem [29], which is in terms of Laplace transforms, instead of its consequences for Dirichlet series [30].

According to Theorem 2.1, a division algebra  $D$  over  $k$  is uniquely specified by its Hasse invariants (i.e., the set  $S = \text{Ram}(D)$  and the choice of fractions  $\{a_p/m_p\}_{p \in S}$ ). Thus, our task is to count the number of ways of choosing these invariants so that the resulting division algebra  $D$  has dimension  $n^2$  and  $|\text{disc}(D)| \leq x$ . It turns out that this is a difficult problem to attack directly. More natural, from the analytic side, is to first count *all* central simple algebras over  $k$  of dimension  $n^2$ . Isolating the count of division algebras can then be obtained by the inclusion-exclusion principle. We now carefully execute the above approach by introducing the following set:

$$N_{m,n}(x) := \#\{\text{central simple algebras } A/k \text{ of dimension } n^2 \text{ of the form}$$

$$A = M(r, D), \text{ where } \dim(D) = d^2 \text{ for some } d \mid m, \text{ and } |\text{disc}(A)| \leq x\}.$$

The remarks earlier in this paragraph show that in general,  $N_{m,n}(x)$  counts the number of choices for Hasse invariants for which  $\text{lcm}_{\mathfrak{p} \in S}[m_{\mathfrak{p}}]$  divides  $m$  and the product in (2) is bounded by  $x$ . Our key lemma is the following estimate for  $N_{m,n}(x)$ . Note that the special case of the lemma when  $m = n$  provides us with asymptotic behavior for the counting function of all dimension  $n^2$  central simple algebras over  $k$ .

**Lemma 3.2.** *Let  $k/\mathbf{Q}$  be a number field. Let  $n > 1$  be an integer, and let  $\ell$  be the smallest prime factor of  $n$ . Let  $m$  be a divisor of  $n$ . Then as  $x \rightarrow \infty$ ,*

$$N_{m,n}(x) = (\delta_{m,n} + o(1))x^{\frac{1}{n^2(1-1/\ell)}}(\log x)^{\ell-2}$$

for a certain constant  $\delta_{m,n}$ . If  $\ell \nmid m$ , then  $\delta_{m,n} = 0$ . Suppose now that  $\ell \mid m$ . Let  $\kappa$  denote the residue at  $s = 1$  of the Dedekind zeta function  $\zeta_k(s)$ . If  $m$  is odd, then

$$(4) \quad \delta_{m,n} = \frac{\kappa^{\ell-1}}{m(\ell-2)!} \cdot \frac{1}{(n^2(1-1/\ell))^{\ell-2}} \cdot \sum_{\substack{0 \leq j < m \\ \ell \nmid j}} \left( \prod_{\substack{\mathfrak{p} \text{ finite}}} \left( 1 + \frac{\ell-1}{|\mathfrak{p}|} + \sum_{\substack{m_{\mathfrak{p}} \mid m \\ m_{\mathfrak{p}} > \ell}} \frac{\mu(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}},j)})\varphi(m_{\mathfrak{p}})/\varphi(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}},j)})}{|\mathfrak{p}|^{(1-1/m_{\mathfrak{p}})/(1-1/\ell)}} \right) \left( 1 - \frac{1}{|\mathfrak{p}|} \right)^{\ell-1} \right).$$

If  $m$  is even, (4) needs to be multiplied by  $2^{r_1}$ , where  $r_1$  is the number of real embeddings of  $k$ .

Broadly, the proof of the above lemma proceeds as follows. We first set up the count for the algebras and produce corresponding Dirichlet series. We then verify that our Dirichlet series satisfy (i)-(iv) of Theorem 3.1. We complete the proof via Theorem 3.1. The latter two steps comprise the bulk of the work.

*Proof.* We first set up a formal count of the algebras via local invariants. To that end, we will use the orthogonality relations among the roots of unity in an essential way. For each  $d$  dividing  $m$ , we introduce the set

$$\mathfrak{F}(m, d) := \left\{ 1 \leq k \leq m : \frac{k}{m} \text{ has lowest terms denominator } d \right\}.$$

For  $0 \leq j < m$ , let  $\zeta_j = e^{2\pi i j/m}$ , and consider the formal expression

$$\frac{1}{m} \left( \sum_{0 \leq j < m} \left[ \prod_{\substack{\mathfrak{p} \text{ finite}}} \left( 1 + \sum_{\substack{m_{\mathfrak{p}} \mid m \\ m_{\mathfrak{p}} > 1}} \frac{\sum_{a_{\mathfrak{p}} \in \mathfrak{F}(m, m_{\mathfrak{p}})} \zeta_j^{a_{\mathfrak{p}}}}{\mathfrak{p}^{n^2(1-1/m_{\mathfrak{p}})s}} \right) \prod_{\substack{\mathfrak{p} \text{ real} \\ 2 \nmid m}} \left( 1 + \frac{\zeta_j^{m/2}}{\mathfrak{p}^s} \right) \right] \right),$$

where the conditions on the final product mean that this product appears only when  $m$  is even. Expanding, we obtain a formal sum of terms  $a_{\mathfrak{m}}/\mathfrak{m}^s$ , where  $\mathfrak{m}$  ranges over the moduli of  $k$ . Here the coefficient  $a_{\mathfrak{m}}$  counts the number of choices of Hasse invariants for which  $\text{lcm}_{\mathfrak{p} \in S}[m_{\mathfrak{p}}]$  divides  $m$  and

$$\left( \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} \in S}} \mathfrak{p} \right) \left( \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in S}} \mathfrak{p}^{n^2(1-1/m_{\mathfrak{p}})} \right) = \mathfrak{m}.$$

There is a one-to-one correspondence between these choices of Hasse parameters and central simple algebras  $A/k$  of dimension  $n^2$  of the form  $M(r, D)$ , where  $\dim(D) = d^2$  for some  $d \mid m$ , and  $\text{disc}(A) = \mathfrak{m}$ . Since

$d = \text{lcm}[m_p]$  and  $r = n/d$ , we can view the coefficients  $a_m$  as counting these central simple algebras. Thus,

$$N_{m,n}(x) = \sum_{|m| \leq x} a_m.$$

In order to apply Delange's theorem, Theorem 3.1, we need Dirichlet series. We obtain the needed series by simply replacing the primes  $p$  with their norms  $|p|$  in the above products. For  $j = 0, 1, 2, \dots, m-1$ , the Dirichlet series  $G_j(s)$  is given by the following product expansion:

$$(5) \quad G_j(s) = \prod_{p \text{ finite}} \left( 1 + \sum_{\substack{m_p | m \\ m_p > 1}} \frac{\sum_{a_p \in \mathfrak{F}(m, m_p)} \zeta_j^{a_p}}{|p|^{n^2(1-1/m_p)s}} \right) \prod_{\substack{p \text{ real} \\ 2 | m}} \left( 1 + \frac{\zeta_j^{m/2}}{|p|^s} \right).$$

If we then set

$$G(s) = \frac{1}{m} \sum_{0 \leq j < m} G_j(s),$$

the coefficient of  $N^{-s}$  in  $G(s)$  is precisely  $\sum_{|m|=N} a_m$ . Hence,  $N_{m,n}(x)$  is precisely the partial sum up to  $x$  of the coefficients of  $G(s)$ .

We now establish that our Dirichlet series satisfy the conditions of Theorem 3.1.

**Claim.**  $G(s)$  satisfies (i)-(iv) of Theorem 3.1.

*Proof of Claim.* Since the coefficients of  $G(s)$  count central simple algebras, their non-negativity is obvious. This shows that condition (i) of Delange's theorem is satisfied. To verify conditions (ii)-(iv) for  $G(s)$ , it suffices to verify that they hold for each individual  $G_j(s)$ . We will show this with

$$(6) \quad \rho = \frac{1}{n^2(1-1/\ell)} \quad \text{and} \quad \beta = \ell - 1.$$

Proceeding further requires a careful study of the product definition (5) of  $G_j(s)$ . First, we deal with the product over real primes, which is present only when  $2 | m$ . By our convention that real primes have norm 1,

$$\left( 1 + \frac{\zeta_j^{m/2}}{|p|^s} \right) = (1 + \zeta_j^{m/2})^{r_1};$$

in particular, this factor is independent of  $s$ . For all finite primes  $p$ , the  $p$ th term in (5) has the form  $1 + A_p(s)$ , where

$$(7) \quad A_p(s) = \sum_{\substack{m_p | m \\ m_p > 1}} \frac{\sum_{a_p \in \mathfrak{F}(m, m_p)} \zeta_j^{a_p}}{|p|^{n^2(1-1/m_p)s}}.$$

Since  $m$  divides  $n$  and  $\ell$  is the least prime divisor of  $n$ , we have

$$n^2(1-1/m_p) \geq n^2(1-1/\ell)$$



for each term in the sum. Moreover, each numerator on the right-hand side of (7) is trivially bounded by  $m$ . It follows that the formal Dirichlet series expansion of  $G_j(s)$  converges absolutely for

$$\Re(s) > \frac{1}{n^2(1-1/\ell)}$$

and coincides there with its (absolutely convergent) Euler product. This gives condition (ii). In fact, if  $\ell \nmid m$ , then the smallest nontrivial divisor of  $m$  is strictly larger than  $\ell$ . The argument of the preceding paragraph then implies that  $G_j(s)$  has an Euler product converging absolutely and uniformly in

$$\Re(s) > \frac{1}{n^2(1-1/\ell)} - \varepsilon,$$

for some positive  $\varepsilon$ . This shows that conditions (iii) and (iv) hold for  $G_j(s)$ , where in (iv) we may take  $A(s) = 0$  and  $B(s) = G_j(s)$ .

In the case when  $\ell \mid m$ , we have to analyze the  $A_p(s)$  more closely. For each  $m_p$  dividing  $m$ , the corresponding numerator on the right-hand side of (7) coincides with the Ramanujan sum  $c_{m_p}(j)$ . From Hölder's explicit evaluation of such sums,

$$\sum_{a_p \in \mathfrak{F}(m, m_p)} \zeta_j^{a_p} = \mu\left(\frac{m_p}{(\ell, j)}\right) \frac{\varphi(m_p)}{\varphi(m_p/(\ell, j))}.$$

Thus, the first term on the right-hand sum in (7) — corresponding to  $m_p = \ell$  — is

$$\mu\left(\frac{\ell}{(\ell, j)}\right) \frac{\ell-1}{\varphi(\ell/(\ell, j))} \frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}}.$$

For all of the remaining terms,

$$n^2(1-1/m_p) > n^2(1-1/\ell).$$

Now if  $\ell \nmid j$ ,

$$\mu\left(\frac{\ell}{(\ell, j)}\right) \frac{\ell-1}{\varphi(\ell/(\ell, j))} \frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}} = -\frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}}.$$

Comparing Euler products term-by-term, it follows that for

$$\Re(s) > \frac{1}{n^2(1-1/\ell)},$$

we have

$$G_j(s) = \zeta_k(n^2(1-1/\ell)s)^{-1} H_j(s),$$

for a certain  $H_j(s)$  analytic for

$$\Re(s) \geq \frac{1}{n^2(1-1/\ell)}.$$

Since  $\zeta_k(s)$  has no zeros on  $\Re(s) = 1$ , this gives an analytic continuation of  $G_j(s)$  to

$$\Re(s) \geq \frac{1}{n^2(1-1/\ell)}.$$

This proves (iii) and (iv) with  $A(s) = 0$  and  $B(s) = G_j(s)$ . Now suppose that  $\ell \mid j$ . Then

$$\mu\left(\frac{\ell}{(\ell, j)}\right) \frac{\ell-1}{\varphi(\ell)/\varphi((\ell, j))} \frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}} = \frac{\ell-1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}}.$$

In this case, comparing Euler products shows that for

$$\Re(s) > \frac{1}{n^2(1-1/\ell)},$$

we have

$$G_j(s) = \zeta_k(n^2(1-1/\ell)s)^{\ell-1} H_j(s),$$

where  $H_j(s)$  is analytic in the half plane

$$\Re(s) \geq \frac{1}{n^2(1-1/\ell)}.$$

This shows that  $G_j(s)$  continues analytically to the same closed half-plane, except for a pole of order at most  $\ell-1$  at

$$s = \frac{1}{n^2(1-1/\ell)}.$$

Consequently, (iii) and (iv) hold with

$$A(s) = G_j(s) \left( s - \frac{1}{n^2(1-1/\ell)} \right)^{\ell-1}$$

and  $B(s) = 0$ . Collecting everything, we see that assumptions (i)–(iv) all hold for  $G(s)$ , for  $\rho$  and  $\beta$  as in (6). Moreover, we can take the  $A(s)$  in (iv) corresponding to  $G(s)$  as  $\frac{1}{m}$  times the sum of the functions  $A(s)$  corresponding to each  $G_j(s)$ .  $\square$

We now establish the lemma with a few applications of Theorem 3.1. We split into two cases.

**Case 1.**  $\ell \nmid m$ .

In the case when  $\ell \nmid m$ , the  $A(s)$  corresponding to each  $G_j(s)$  was identically zero, hence our final  $A(s)$  is also 0. Thus, Theorem 3.1 yields

$$N_{m,n}(x) = o(x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2}),$$

as  $x \rightarrow \infty$ . This completes the proof of the lemma in the case  $\ell \nmid m$ .

**Case 2.**  $\ell \mid m$ .

If  $\ell \mid m$ , our work shows that

$$A(s) = \left( s - \frac{1}{n^2(1-1/\ell)} \right)^{\ell-1} \cdot \frac{1}{m} \left( \sum_{\substack{0 \leq j < m \\ \ell \mid j}} G_j(s) \right).$$

To evaluate this  $A(s)$  at

$$s = \frac{1}{n^2(1-1/\ell)},$$

we recall that  $\kappa$  denotes the residue at  $s = 1$  of the simple pole of  $\zeta_k(s)$ . Writing

$$\left(s - \frac{1}{n^2(1-1/\ell)}\right)^{\ell-1} G_j(s) = \left(\zeta_k(n^2(1-1/\ell)s) \left(s - \frac{1}{n^2(1-1/\ell)}\right)\right)^{\ell-1} \cdot G_j(s) \zeta_k(n^2(1-1/\ell)s)^{-(\ell-1)},$$

we see that

$$A\left(\frac{1}{n^2(1-1/\ell)}\right) = \left(\frac{\kappa}{n^2(1-1/\ell)}\right)^{\ell-1} \cdot \frac{1}{m} \left[ \sum_{\substack{0 \leq j < m \\ \ell \mid j}} \left( \lim_{s \rightarrow \frac{1}{n^2(1-1/\ell)}} G_j(s) \zeta_k(n^2(1-1/\ell)s)^{-(\ell-1)} \right) \right].$$

It remains to evaluate the limits inside the final sum. For the values of  $j$  and  $m$  under consideration,  $\ell \mid j$  and  $\ell \mid m$ . So for each finite prime  $\mathfrak{p}$ , the  $\mathfrak{p}$ th term in the product expansion (5) of  $G_j(s)$  begins as

$$1 + (\ell-1)/|\mathfrak{p}|^{m^2(1-1/\ell)s} + \dots$$

Now consider the factors corresponding to infinite primes. If  $m$  is odd, then there are no such factors in (5). If  $m$  is even, then we must have  $\ell = 2$ , and since  $\ell \mid j$ ,

$$1 + \zeta_j^{m/2} = 1 + e^{\pi i j} = 1 + (-1)^j = 2;$$

thus, the factor in (5) giving the contribution of the infinite primes is precisely  $2^{r_1}$ . We conclude that if  $m$  is odd, then

$$\lim_{s \rightarrow \frac{1}{n^2(1-1/\ell)}} G_j(s) \zeta_k(s)^{-(\ell-1)} = \prod_{\mathfrak{p} \text{ finite}} \left( 1 + \frac{\ell-1}{|\mathfrak{p}|} + \sum_{\substack{m_{\mathfrak{p}} \mid m \\ m_{\mathfrak{p}} > \ell}} \frac{\mu\left(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}}, j)}\right) \frac{\varphi(m_{\mathfrak{p}})}{\varphi(m_{\mathfrak{p}}/(m_{\mathfrak{p}}, j))}}{|\mathfrak{p}|^{(1-1/m_{\mathfrak{p}})/(1-1/\ell)}} \right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1},$$

while if  $m$  is even, this must be multiplied by  $2^{r_1}$ . So if  $m$  is odd, then

$$A\left(\frac{1}{n^2(1-1/\ell)}\right) = \left(\frac{\kappa}{n^2(1-1/\ell)}\right)^{\ell-1} \cdot \frac{1}{m} \cdot \sum_{\substack{0 \leq j < m \\ \ell \mid j}} \left( \prod_{\mathfrak{p} \text{ finite}} \left( 1 + \frac{\ell-1}{|\mathfrak{p}|} + \sum_{\substack{m_{\mathfrak{p}} \mid m \\ m_{\mathfrak{p}} > \ell}} \frac{\mu\left(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}}, j)}\right) \frac{\varphi(m_{\mathfrak{p}})}{\varphi(m_{\mathfrak{p}}/(m_{\mathfrak{p}}, j))}}{|\mathfrak{p}|^{(1-1/m_{\mathfrak{p}})/(1-1/\ell)}} \right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} \right),$$

while if  $m$  is even, this expression should be multiplied by  $2^{r_1}$ . According to Theorem 3.1, we have

$$(8) \quad N_{m,n}(x) = \left( \frac{A\left(\frac{1}{n^2(1-1/\ell)}\right)}{\frac{1}{n^2(1-1/\ell)} \Gamma(\ell-1)} + o(1) \right) x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2},$$

as  $x \rightarrow \infty$ . Comparing Equation (8) with the definition of  $\delta_{m,n}$  in the statement of the lemma, we see the proof is complete.  $\square$

We now prove Theorem 1.5 from the introduction.

*Proof of Theorem 1.5.* We view  $N(x)$  as counting central simple algebras of the form  $M(r, D)$  where  $r = 1$ . To single these out, we make use of the well-known identity

$$\sum_{d|r} \mu(d) = 1$$

if  $r = 1$  and 0 otherwise. Writing  $\sum_A$  for a sum on central simple algebras  $A$  of dimension  $n^2$ , and  $\sum_A^{(r)}$  for such a sum restricted to  $A$  of the form  $M(r, D)$ , we find that

$$N(x) = \sum_A^{(1)} 1 = \sum_{m|r} \mu(m) \sum_{\substack{r|n \\ m|r}} \sum_A^{(r)} 1.$$

Writing  $r^2 \dim(D) = n^2$ , we see that  $m$  divides  $r$  if and only if  $\dim(D) = d^2$  for divisor  $d$  of  $n/m$ . Hence,

$$\sum_{\substack{r|n \\ m|r}} \sum_A^{(r)} 1 = N_{n/m,n}(x).$$

Putting the last two displays together, we find that

$$N(x) = \sum_{m|n} \mu(m) N_{n/m,n}(x).$$

Replacing  $m$  with  $n/m$  gives the first statement in the lemma. The asymptotic formula (1) with

$$\delta_n = \sum_{m|n} \mu(n/m) \delta_{m,n}$$

now follows from Lemma 3.2.

It remains to show that  $\delta_n > 0$ . Consider first the case when  $n = \ell$  is prime. In that case,

$$\delta_n = \delta_{\ell,n} - \delta_{1,n} = \delta_{\ell,n}.$$

We used here that  $\delta_{1,n} = 0$  since  $\ell \nmid 1$ . From Lemma 3.2,  $\delta_{\ell,n}$  is given by a product of obviously nonzero factors together with

$$\prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1}.$$

This final product is absolutely convergent and contains only nonzero terms, and so also represents a nonzero real number. This settles the case when  $n = \ell$ .

Now we treat the case of general  $n$ . Fix finite primes  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  of  $k$ . We count division algebras  $A/k$  of dimension  $\ell^2$  which are unramified at any of  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  and which satisfy  $\text{disc}(A) \leq X$ . Without the ramification condition, we have just seen that the number of these  $A$  is

$$(9) \quad \gg X^{\frac{1}{\ell^2(1-1/\ell)}} (\log X)^{\ell-2}$$

for large  $X$ . An entirely analogous proof shows that this lower bound continues to hold with the restrictions on ramification imposed. Now for each such  $A$ , there is an associated  $n^2$ -dimensional division algebra  $A'$  over  $k$  specified by enlarging  $\mathcal{P}$  to include  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ , and letting  $a_{\mathfrak{p}_i}/m_{\mathfrak{p}_i} = 1/n$ . Moreover,

$$|\text{disc}(A')| = |\mathfrak{p}_1 \cdots \mathfrak{p}_n|^{n^2(1-1/n)} |\text{disc}(A)|^{(n/\ell)^2}.$$

The number of  $n^2$ -dimensional algebras  $A'$  constructed in this way, with discriminant having norm up to  $x$ , satisfies the lower bound (9) with

$$X := (x/|\mathfrak{p}_1 \cdots \mathfrak{p}_n|^{n^2(1-1/n)})^{(\ell/n)^2},$$

which is

$$\gg x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2}$$

for all large  $x$ . This is only possible if  $\delta_n > 0$  in (1).  $\square$

*Examples 1.* The explicit expression for  $\delta_n$  is, in general, exceedingly complicated. However, it can be written fairly compactly in certain special cases. To begin with, suppose that the smallest prime factor  $\ell$  of  $n$  is odd. If  $n = \ell$ , then  $\delta = \delta_{\ell,n}$ , where

$$(10) \quad \delta_{\ell,n} = \frac{\kappa^{\ell-1}}{\ell(\ell-2)!} \frac{1}{(n^2(1-1/\ell))^{\ell-2}} \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1}.$$

Next, suppose that  $n = \ell^2$ . Then

$$\delta_n = \delta_{\ell^2, \ell^2} - \delta_{\ell, \ell^2}.$$

The second term can be calculated with (10), while

$$\begin{aligned} \delta_{\ell^2, \ell^2} &= \frac{\kappa^{\ell-1}}{\ell^2(\ell-2)!} \cdot \frac{1}{(\ell^4(1-1/\ell))^{\ell-2}} \cdot \\ &\quad \left( \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|} + \frac{\ell(\ell-1)}{|\mathfrak{p}|^{1+1/\ell}}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} + \right. \\ &\quad \left. (\ell-1) \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|} - \frac{\ell}{|\mathfrak{p}|^{1+1/\ell}}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} \right). \end{aligned}$$

Finally, suppose that  $n = \ell\ell'$ , where  $\ell'$  is a prime larger than  $\ell$ . Then

$$\delta_n = \delta_{\ell\ell', \ell\ell'} - \delta_{\ell, \ell\ell'} - \delta_{\ell', \ell\ell'},$$

where the second and third terms can be computed with (10), and

$$\begin{aligned} \delta_{\ell\ell'} &= \frac{\kappa^{\ell-1}}{\ell\ell'(\ell-2)!} \cdot \frac{1}{(\ell^2\ell'^2(1-1/\ell))^{\ell-2}} \cdot \\ &\quad \left( \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|} + \frac{\ell'-1}{|\mathfrak{p}|^{\frac{1-1/\ell'}{1-1/\ell}}} + \frac{\ell(\ell-1)}{|\mathfrak{p}|^{1+1/\ell}}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} + \right. \\ &\quad \left. (\ell'-1) \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|} - \frac{1}{|\mathfrak{p}|^{\frac{1-1/\ell'}{1-1/\ell}}} - \frac{\ell'-1}{|\mathfrak{p}|^{1+1/\ell}}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} \right). \end{aligned}$$

If the least prime factor of  $n$  is  $\ell = 2$ , the same analysis applies, but all of these expressions for  $\delta_n$  must be multiplied by  $2^{r_1}$ .

**3.2. Theorem 1.6: Counting quadratic extensions that embed into a fixed quaternion algebra.** In this section, we fix a number field  $k$  and a quaternion algebra  $B$  defined over  $k$  and count the number of quadratic extensions  $L/k$  with norm of relative discriminant less than  $X$  which embed into  $B$ . In what follows, denote by  $\Delta_{L/k}$  the relative discriminant of  $L$  over  $k$ . If  $P$  is any property a quadratic extension of  $k$  may have, we make the definition

$$(11) \quad \mathbf{Prob}(P) := \lim_{x \rightarrow \infty} \frac{\#\{\text{quadratic extensions } L/k \text{ for which } P \text{ holds and } |\Delta_{L/k}| \leq x\}}{\#\{\text{quadratic extensions } L/k \text{ with } |\Delta_{L/k}| \leq x\}},$$

provided that this limit exists. The next result, which is a special case of results of Wood [95], asserts that for certain properties  $P$  related to splitting behavior, these “probabilities” behave as one might naively expect.

**Proposition 3.3** (Wood). *Fix a finite collection  $S$  of real or finite places of  $k$ . For each  $\mathfrak{p} \in S$ , let  $P_{\mathfrak{p}}$  be one of the properties “ $\mathfrak{p}$  ramifies in  $L$ ”, “ $\mathfrak{p}$  splits in  $L$ ”, or “ $\mathfrak{p}$  is inert in  $L$ ”, subject to the restriction that  $P_{\mathfrak{p}}$  is one of the first two if  $\mathfrak{p}$  is a real place. Then:*

- (i)  $\mathbf{Prob}(P_{\mathfrak{p}})$  exists for each  $\mathfrak{p} \in S$ .
- (ii)  $\mathbf{Prob}(\text{all } P_{\mathfrak{p}} \text{ hold at once}) = \prod_{\mathfrak{p} \in S} \mathbf{Prob}(P_{\mathfrak{p}})$ .
- (iii) If  $\mathfrak{p}$  is real, then  $\mathbf{Prob}(\mathfrak{p} \text{ ramifies}) = \mathbf{Prob}(\mathfrak{p} \text{ splits}) = \frac{1}{2}$ .
- (iv) If  $\mathfrak{p}$  is finite, then

$$\mathbf{Prob}(\mathfrak{p} \text{ splits}) = \mathbf{Prob}(\mathfrak{p} \text{ is inert}) = \frac{1}{2}(1 - \mathbf{Prob}(\mathfrak{p} \text{ ramifies})).$$

It is worth saying a few words about how Proposition 3.3 follows from the much more general results of Wood. In Wood’s terminology, we are counting  $\mathbf{Z}/2\mathbf{Z}$ -extensions of  $k$  with local specifications. We note however that Wood’s definition of a local specification differs from our simplified picture above, but only in the sense that it is strictly finer; she allows one to specify the  $k$ -algebra  $L \otimes_k k_{\mathfrak{p}}$ , which gives us more information than we are measuring. When  $G = \mathbf{Z}/2\mathbf{Z}$ , all local specifications are viable (see [95, start of §2.2]), and counting by discriminant defines a fair counting function (in the sense of [95, §2.1]). The existence of each  $\mathbf{Prob}(P_{\mathfrak{p}})$  in Proposition 3.3 can now be seen as a special case of [95, Theorem 2.1]. The independence result follows from [95, Corollary 2.4]. The statement about the splitting behavior of real primes comes from [95, Corollary 2.2], while the statement about the behavior of finite primes is guaranteed by [95, Corollary 2.3].

Theorem 1.6 follows easily from Proposition 3.3 and the following estimate of Datskovsky and Wright [27] for the denominator appearing in the definition (11) (see [24, §2.2] for an alternative proof of this proposition).

**Proposition 3.4.** *The number of quadratic extensions  $L/k$  with  $|\Delta_{L/k}| \leq x$  is*

$$\sim \frac{1}{2^{r_2}} \frac{\kappa_k}{\zeta_k(2)} x,$$

as  $x \rightarrow \infty$ , where  $\kappa_k$  denotes the residue at  $s = 1$  of  $\zeta_k(s)$  and  $r_2$  is the number of pairs of complex embeddings of  $k$ .



*Deduction of Theorem 1.6.* Recall that  $L$  embeds into  $B$  precisely when every prime dividing the discriminant of  $B$  is non-split in  $L$ . The probability that a fixed real prime of  $k$  ramifies in  $L$  is  $\frac{1}{2}$  (from Proposition 3.3(iii)), while the probability that a fixed finite prime of  $k$  is inert or ramified in  $L$  is (from Proposition 3.3(iv))

$$\frac{1}{2}(1 + \mathbf{Prob}(\mathfrak{p} \text{ ramifies})) \geq \frac{1}{2}.$$

So from Proposition 3.3(ii), the probability that  $L$  embeds into  $B$  exists and is at least  $\frac{1}{2^{r'}}$ , where  $r'$  is the number of distinct places dividing the discriminant of  $B$ . Theorem 1.6 now follows from the estimate of Proposition 3.4.  $\square$

**3.3. Theorem 1.7: Counting quaternion algebras admitting fixed embeddings.** For a number field  $k$  and a quadratic extension  $L/k$ , our present goal is to count the number of quaternion algebras over  $k$  which have discriminant less than  $x$  and which admit an embedding of  $L$ . In fact, we solve a more general problem. Specifically, in this subsection we prove Theorem 1.7 from the introduction.

**3.3.1. Setup.** From Theorem 2.1, a quaternion algebra  $B/k$  is uniquely specified by a finite set  $S \subset \mathcal{P}_k$  of real and finite places of  $k$ , along with a reduced fraction  $0 < a_{\mathfrak{p}}/m_{\mathfrak{p}} < 1$  for each prime  $\mathfrak{p} \in S$ , where  $\text{lcm}_{\mathfrak{p} \in S}[m_{\mathfrak{p}}] = 2$  and

$$\sum_{\mathfrak{p} \in S} a_{\mathfrak{p}}/m_{\mathfrak{p}} \in \mathbf{Z}.$$

The least common multiple condition forces each  $a_{\mathfrak{p}}/m_{\mathfrak{p}} = 1/2$ , and the integrality condition on the sum forces the cardinality of  $S$  to be even. We conclude that there is a bijection between quaternion algebras over  $k$  and square-free moduli  $\mathfrak{m}$  of  $k$  containing a nonzero even number of factors. Moreover, if  $B$  corresponds to  $\mathfrak{m}$  under this bijection, then

$$\text{disc}(B) = \left( \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} | \mathfrak{m}}} \mathfrak{p} \right)^2 \cdot \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} | \mathfrak{m}}} \mathfrak{p}.$$

Now let  $\mathcal{Q}$  be the set of finite or real primes of  $k$  that do not split in any of the  $L_i$ . Asking that all of our quadratic extensions  $L_i$  embed into the quaternion algebra  $B/k$  amounts to requiring that  $\mathfrak{m}$  only be divisible by primes residing in  $\mathcal{Q}$ . We count the number of such  $B$  with  $|\text{disc}(B)| \leq x$  by modifying the approach of the last section. We now provide the details. Define

$$G(s) = \frac{1}{2}(G_0(s) + G_1(s)),$$

where

$$(12) \quad G_0(s) = \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} \in \mathcal{Q}}} \left( 1 + \frac{1}{|\mathfrak{p}|^s} \right) \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in \mathcal{Q}}} \left( 1 + \frac{1}{|\mathfrak{p}|^{2s}} \right)$$

and

$$(13) \quad G_1(s) = \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} \in \mathcal{Q}}} \left( 1 - \frac{1}{|\mathfrak{p}|^s} \right) \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in \mathcal{Q}}} \left( 1 - \frac{1}{|\mathfrak{p}|^{2s}} \right).$$

The infinite factors in the definitions of  $G_0(s)$  and  $G_1(s)$  are in fact independent of  $s$ . If  $r'_1$  is the number of real primes of  $k$  that do not split in any of the  $L_i$ , the contribution of the infinite factors is given by  $2^{r'_1}$  and  $0^{r'_1}$ , respectively, where

$$0^{r'_1} = \begin{cases} 1, & r'_1 = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Now observe that if  $G(s)$  is identified with its formal Dirichlet series expansion, then the coefficient of  $N^{-s}$  counts quaternion algebras  $B/k$  with  $|\text{disc}(B)| = N$  admitting an embedding of all  $L_i$ .

To estimate the partial sums of the  $G(s)$ -coefficients for  $N \leq x$ , we work with the corresponding sums for  $G_0(s)$  and  $G_1(s)$  individually. For  $G_0(s)$ , we will apply Theorem 3.1 to obtain an asymptotic formula with main term proportional to

$$x^{1/2}/(\log x)^{1-\frac{1}{2r}}.$$

We then use a result of Wirsing [94, Satz 2] to show that the partial sums of the  $G_1$ -coefficients are in fact

$$o(x^{1/2}/(\log x)^{1-\frac{1}{2r}}),$$

as  $x \rightarrow \infty$ . Putting these estimates together yields Theorem 1.7.

**3.3.2. The partial sums of the coefficients of  $G_0(s)$ .** Let us check that the hypotheses of Theorem 3.1 hold with  $\rho = \frac{1}{2}$  and  $\beta = \frac{1}{2r}$ . Conditions (i) and (ii) of that theorem are clear from the product definition of  $G_0$ , and so we may focus on (iii) and (iv). Here the essential idea is to express  $G_0(s)$  in terms of benign factors and Artin  $L$ -functions attached to  $\text{Gal}(L/k)$ . We now implement this idea. Our assumption that

$$[L_1 \cdots L_r : k] = 2^r$$

easily implies that  $\text{Gal}(L/k)$  is canonically isomorphic to the elementary abelian 2-group

$$\bigoplus_{i=1}^r \text{Gal}(L_i/k) = \bigoplus_{i=1}^r \mathbf{Z}/2\mathbf{Z} = (\mathbf{Z}/2\mathbf{Z})^r.$$

For  $1 \leq i \leq r$ , let  $\tilde{\chi}_i$  denote the unique character of  $\text{Gal}(L/k)$  whose kernel is the subgroup fixing  $L_i$ . For every subset  $T$  of  $\{1, \dots, r\}$ , let

$$\tilde{\chi}_T = \prod_{i \in T} \tilde{\chi}_i.$$

It is a simple matter that  $\tilde{\chi}_T$  is nontrivial provided  $T$  is non-empty. Consequently, the field  $L_T$  left fixed by  $\ker \tilde{\chi}_T$  is a quadratic extension of  $k$  in the event  $T$  is non-empty. For each finite prime  $\mathfrak{p}$  of  $k$ , we let  $\chi_T(\mathfrak{p}) = 1, 0$ , or  $-1$  according to whether  $\mathfrak{p}$  splits, ramifies, or remains inert in  $L_T$ . When  $T$  consists of a single element  $1 \leq i \leq r$ , we will write  $\chi_i$  instead of the more cumbersome  $\chi_{\{i\}}$ . In that notation, unless  $\mathfrak{p}$  belongs to

$$\mathcal{R} := \{\text{finite primes of } k \text{ that ramify in } L\},$$

we have the expression

$$\chi_T(\mathfrak{p}) = \tilde{\chi}_T(\text{Frob}(\mathfrak{p})) = \prod_{i \in T} \tilde{\chi}_i(\text{Frob}(\mathfrak{p})) = \prod_{i \in T} \chi_i(\mathfrak{p}),$$

where  $\text{Frob}(\mathfrak{p}) \in \text{Gal}(L/k)$  is the associated Frobenius automorphism for  $\mathfrak{p}$ .

Now we relate the  $\chi_i$  to the definition of  $G_0$ . If  $\mathfrak{p}$  is finite and not an element of  $\mathcal{R}$ , then

$$\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p})) = 1$$

if  $\mathfrak{p} \in \mathcal{Q}$  and  $= 0$  otherwise. Hence, setting  $\mathcal{Q}_0 := \mathcal{Q} \cap \mathcal{R}$ , we have the expression

$$(14) \quad G_0(s) = 2^{r'} \prod_{\mathfrak{p} \in \mathcal{Q}_0} \left( 1 + \frac{1}{|\mathfrak{p}|^{2s}} \right) \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{R}}} \left( 1 + \frac{\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p}))}{|\mathfrak{p}|^{2s}} \right).$$

For  $\mathfrak{p} \notin \mathcal{R}$ , we have

$$\prod_{i=1}^r (1 - \chi_i(\mathfrak{p})) = \sum_{T \subset \{1, 2, \dots, r\}} (-1)^{\#T} \chi_T(\mathfrak{p}).$$

Let

$$Z_0(s) := \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{R}}} \left( \left( 1 + \frac{\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p}))}{|\mathfrak{p}|^{2s}} \right)^{2^r} \prod_{T \subset \{1, 2, \dots, r\}} \left( 1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|^{2s}} \right)^{(-1)^{\#T}} \right).$$

Recalling the Maclaurin series for  $\log(1+t)$ , we see that  $\log Z_0(s)$  can be represented as a Dirichlet series that converges absolutely and uniformly on compact subsets of  $\Re(s) > \frac{1}{4}$ . Hence,  $Z_0(s)$  can be extended to an analytic and nonzero function there.

For each  $T \subset \{1, 2, \dots, r\}$  and all  $s$  with real part greater than 1, put

$$L(s, \chi_T) = \prod_{\mathfrak{p} \text{ finite}} \left( 1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|^s} \right)^{-1}.$$

$L(s, \chi_T)$  is the Artin  $L$ -function attached to the character  $\chi_T$  of  $\text{Gal}(L/k)$ . When  $T = \emptyset$ , we have  $L(s, \chi_T) = \zeta_k(s)$ , and for all other choices of  $T$ , the function  $L(s, \chi_T)$  is analytic and nonzero for  $\Re(s) \geq 1$ .

We chose  $Z_0(s)$  so that

$$\prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{R}}} \left( 1 + \frac{\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p}))}{|\mathfrak{p}|^{2s}} \right)^{2^r} = Z_0(s) \prod_{T \subset \{1, 2, \dots, r\}} \left( L(2s, \chi_T) \prod_{\mathfrak{p} \in \mathcal{R}} \left( 1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|^{2s}} \right) \right)^{(-1)^{\#T}}.$$

The right-hand products over  $\mathfrak{p} \in \mathcal{R}$  are analytic and nonzero for  $\Re(s) > 0$ . Moreover, the expression

$$(15) \quad \left( s - \frac{1}{2} \right) Z_0(s) \prod_{T \subset \{1, 2, \dots, r\}} \left( L(2s, \chi_T) \prod_{\mathfrak{p} \in \mathcal{R}} \left( 1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|^{2s}} \right) \right)^{(-1)^{\#T}}$$

is analytic and nonzero for  $\Re(s) \geq \frac{1}{2}$ . We note for the reader that the factor of  $s - \frac{1}{2}$  here is used to cancel the simple pole of  $\zeta_k(2s)$  at  $s = \frac{1}{2}$ . Thus, we can extract a  $2^r$ th root  $H_0(s)$  of (15) which is also analytic and

nonzero in  $\Re(s) \geq \frac{1}{2}$ . The choice of  $H_0$  is uniquely specified if we insist that  $H_0(s) > 0$  for  $s > \frac{1}{2}$ . Referring back to (14), we find that for  $\Re(s) > \frac{1}{2}$ ,

$$G_0(s) = \frac{1}{(s - \frac{1}{2})^{1/2r}} \left( 2^{r'_1} \cdot \prod_{\mathfrak{p} \in \mathcal{Q}_0} \left( 1 + \frac{1}{|\mathfrak{p}|^{2s}} \right) \cdot H_0(s) \right),$$

where  $(s - \frac{1}{2})^{1/2r}$  is the principal  $2r$ th root. This immediately implies (iii). If we let

$$A_0(s) := 2^{r'_1} \cdot \prod_{\mathfrak{p} \in \mathcal{Q}_0} \left( 1 + \frac{1}{|\mathfrak{p}|^{2s}} \right) \cdot H_0(s),$$

we see that  $G_0(s)$  satisfies (iv) with  $\rho = \frac{1}{2}$ ,  $\beta = \frac{1}{2r}$ ,  $A(s) = A_0(s)$ , and  $B(s) = 0$ .

So by Theorem 3.1, the sum up to  $x$  of the coefficients of  $G_0(s)$  is asymptotic to

$$\frac{A_0(\frac{1}{2})}{\frac{1}{2}\Gamma(\frac{1}{2r})} x^{\frac{1}{2}} / (\log x)^{1 - \frac{1}{2r}},$$

as  $x \rightarrow \infty$ .

**3.3.3. The coefficients of  $G_1(s)$ .** We now show that the contribution from the coefficients of  $G_1(s)$  is negligible. Define arithmetic functions  $a(N)$  and  $b(N)$  by expanding

$$\prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in \mathcal{Q}}} \left( 1 + \frac{1}{|\mathfrak{p}|^s} \right) = \sum_{N=1}^{\infty} \frac{a(N)}{N^s} \quad \text{and} \quad \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in \mathcal{Q}}} \left( 1 - \frac{1}{|\mathfrak{p}|^s} \right) = \sum_{n=1}^{\infty} \frac{b(N)}{N^s}.$$

The functions  $a(N)$  and  $b(N)$  are multiplicative and satisfy  $|b(N)| \leq a(N)$  for all  $N$ . Referring back to the earlier definitions of  $G_0$  and  $G_1$ , we see that the partial sum of the  $G_0(s)$ -coefficients up to  $x$  is given by

$$2^{r_1} \sum_{N \leq \sqrt{x}} a(N),$$

while that of the  $G_1$ -coefficients is given by

$$0^{r_1} \sum_{N \leq \sqrt{x}} b(N).$$

Thus, if we can show that

$$(16) \quad \sum_{N \leq x} b(N) = o \left( \sum_{N \leq x} a(N) \right) \quad \text{as } x \rightarrow \infty,$$

then the partial sums of the  $G_1$ -coefficients are

$$o(x^{1/2} / (\log x)^{1 - \frac{1}{2r}}),$$

as desired. For that task, we use the following result, which is a slight weakening of a theorem of Wirsing [94, Satz 2].

**Proposition 3.5 (Wirsing).** *Let  $a(N)$  be a multiplicative function taking only nonnegative values. Assume*

(i) there is a constant  $\tau > 0$  for which

$$\sum_{p \leq x} a(p) \log p = (\tau + o(1))x,$$

as  $x \rightarrow \infty$ ,

(ii)  $a(p^\ell)$  is bounded uniformly on prime powers  $p^\ell$  with  $\ell \geq 2$ .

Let  $b(N)$  be a complex-valued multiplicative function satisfying  $|b(N)| \leq a(N)$  for all  $N$ . Suppose moreover that

(iii) there is a constant  $\tau' \neq \tau$  with

$$\sum_{p \leq x} b(p) \log p = (\tau' + o(1))x,$$

as  $x \rightarrow \infty$ ,

$$\text{Then } \sum_{N \leq x} b(N) = o\left(\sum_{N \leq x} a(N)\right).$$

To see the validity of Proposition 3.5, we refer the reader to the remarks immediately following Satz 2 for the formulation that we use. These remarks allow us to replace condition (7) in [94, Satz 2] with the simpler condition that  $\tau \neq \tau'$ . We now return to deducing (16).

*Proof of (16).* Let us check that the hypotheses of Proposition 3.5 are satisfied for our choice of  $a(N)$  and  $b(N)$  above. We have

$$\sum_{p \leq x} a(p) \log p = \sum_{p \leq x} \left( \sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ |\mathfrak{p}| = p}} \log |\mathfrak{p}| \right) = \sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ \mathfrak{p} \text{ abs. degree } 1 \\ |\mathfrak{p}| \leq x}} \log |\mathfrak{p}| = \sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ |\mathfrak{p}| \leq x}} \log |\mathfrak{p}| + O(x^{1/2}).$$

Now  $\mathfrak{p} \in \mathcal{Q}$  if and only if  $\mathfrak{p}$  does not split in any of the  $L_i$ . Since

$$\text{Gal}(L/k) \cong \prod_{i=1}^r \text{Gal}(L_i/k),$$

the Chebotarev density theorem (for natural density) yields

$$\sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ |\mathfrak{p}| \leq x}} \log |\mathfrak{p}| = \left( \frac{1}{2^r} + o(1) \right) x,$$

as  $x \rightarrow \infty$ . So (i) holds with  $\tau = \frac{1}{2^r}$ .

For each prime power  $p^\ell$ ,

$$a(p^\ell) \leq \# \left\{ \text{square-free ideals of } \mathcal{O}_k \text{ of norm } p^\ell \right\}.$$

However, any square-free ideal of norm  $p^\ell$  must be a square-free product of the primes lying above  $p$ , and there are at most  $2^{[k:\mathbb{Q}]}$  such products. This gives (ii).

Finally, our work towards (i) shows that

$$\sum_{p \leq x} b(p) \log p = - \sum_{p \leq x} \sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ |\mathfrak{p}| = p}} \log |\mathfrak{p}| = - \left( \frac{1}{2^r} + o(1) \right) x,$$

as  $x \rightarrow \infty$ . Hence, (iii) holds with  $\tau' = -\frac{1}{2^r}$ .  $\square$

3.3.4. *Denouement.* Since

$$G(s) = \frac{1}{2}(G_0(s) + G_1(s)),$$

combining the results of the previous two sections shows that the number of quaternion algebras  $B/k$  admitting embeddings of all of the  $L_i$  and having  $|\text{disc}(B)| \leq x$ , is asymptotically

$$\frac{A_0\left(\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2^r}\right)} \cdot x^{1/2} / (\log x)^{1-\frac{1}{2^r}}.$$

The leading coefficient here is nonzero and can be given explicitly in terms of the leading terms in the Laurent series expansions for the functions  $L(s, \chi_T)$ . Specifically, tracing back through the definitions, we see that with  $\kappa$  equal to the residue at  $s = 1$  of  $\zeta_k(s)$ ,

$$\begin{aligned} \frac{A_0\left(\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2^r}\right)} &= \frac{2^{r'-\frac{1}{2^r}}}{\Gamma\left(\frac{1}{2^r}\right)} \prod_{\mathfrak{p} \in \mathcal{Q}_0} \left(1 + \frac{1}{|\mathfrak{p}|}\right) \cdot \\ &\quad \left( \kappa \prod_{\mathfrak{p} \in \mathcal{Q}} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \prod_{\substack{T \subset \{1, 2, \dots, r\} \\ T \neq \emptyset}} \left( L(1, \chi_T) \prod_{\mathfrak{p} \in \mathcal{Q}} \left(1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|}\right) \right)^{(-1)^{\#T}} \right)^{1/2^r} \cdot Z^{1/2^r}, \end{aligned}$$

where

$$\begin{aligned} Z &:= Z_0 \left( \frac{1}{2} \right) \\ &= \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{Q}}} \left( \left( 1 + \frac{\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p}))}{|\mathfrak{p}|} \right)^{2^r} \prod_{T \subset \{1, 2, \dots, r\}} \left( 1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|} \right)^{(-1)^{\#T}} \right). \end{aligned}$$

It is clear that in general, the explicit form of this leading coefficient is rather complicated, but in the case  $r = 1$  it simplifies nicely to the formula given in Example 1.

**Remark.** Without the assumption that

$$[L_1 \cdots L_r : k] = 2^r,$$

it is possible for there to be *no* quaternion division algebras  $B/k$  into which all of the  $L_i$  embed. For example, take  $k = \mathbf{Q}$  and consider the collection of  $L_i$  given by  $\mathbf{Q}(\sqrt{-3})$ ,  $\mathbf{Q}(\sqrt{-1})$ ,  $\mathbf{Q}(\sqrt{3})$ ,  $\mathbf{Q}(\sqrt{10})$ ,  $\mathbf{Q}(\sqrt{17})$ . One can check that every finite prime of  $\mathbf{Q}$  splits in at least one of these  $L_i$ , and so a quaternion algebra into which all of these fields embeds must have a discriminant not divisible by any finite prime at all. As a quaternion algebra must ramify at a finite even number of primes, we conclude that up to isomorphism the only quaternion algebra admitting embeddings of all of the above extensions is  $\mathbf{M}(2, \mathbf{Q})$ , which is clearly not a division algebra.



For the general situation, we proceed as follows. Suppose we are given a finite collection of distinct quadratic extensions  $L_i/k$ . Let  $L$  be the compositum of all of the  $L_i$ , and define  $r$  by the condition  $[L : k] = 2^r$ . Note, we are not assuming here that  $r$  is the total number of  $L_i$ . For each  $i$ , let  $\tilde{\chi}_i$  be the character of  $\text{Gal}(L/k)$  whose kernel is the subgroup fixing  $L_i$ . For there to be infinitely many quaternion algebras  $B/k$  into which all of the  $L_i$  embed, it is necessary and sufficient that there is no finite **odd order** subset of the  $\tilde{\chi}_i$  which multiply to the identity. If this condition holds, then the number of  $B/k$  with  $|\text{disc}(B)| \leq x$  into which all of the  $L_i$  embed is again asymptotic to

$$\delta x^{1/2} / (\log x)^{1 - \frac{1}{2^r}}$$

for some positive  $\delta > 0$ . This can be established by slight modifications to the proof of Theorem 1.7.

#### 4. MAIN TOOLS: GEOMETRIC COUNTING RESULTS

In this section, we derive the geometric counting results from the introduction using the tools from the previous section.

**4.1. Corollaries 1.8 and 1.9: Counting commensurability classes of manifolds and orbifolds.** As an application to Theorem 1.5 we consider the problem of counting commensurability classes of arithmetic hyperbolic 2– and 3–manifolds with a fixed invariant trace field  $k$ . As Selberg’s lemma ensures every complete, finite volume hyperbolic  $n$ –orbifold has a finite manifold cover, counting commensurability classes of arithmetic orbifolds is the same as counting commensurability classes of arithmetic manifolds. Consequently, we will not fret about whether our representatives are manifolds or orbifolds. It is well-known [65, Chapter 11] that given such a commensurability class  $\mathcal{C}$ , there is a real number  $V_{\mathcal{C}} > 0$  which occurs as the smallest volume achieved by an orbifold belonging to this class. A consequence of Borel’s classification of maximal arithmetic Fuchsian and Kleinian groups and their volumes [7] is that we can derive a precise formula for  $V_{\mathcal{C}}$  in terms of the number theoretic invariants of  $\mathcal{C}$ .

The proofs of Corollary 1.8 and Corollary 1.9 will rely crucially on Theorem 2.5. Namely, every commensurability class of arithmetic hyperbolic 2– or 3–manifolds both determines and is determined by the associated invariant trace field and invariant quaternion algebra.

We begin by proving a lemma which bounds the norm of the discriminant of the invariant quaternion algebra of a compact arithmetic hyperbolic 2– or 3–manifold as a function of the volume  $V$  of the manifold.

**Lemma 4.1.** *Let  $M$  be a compact arithmetic hyperbolic 2–manifold (3–manifold) of volume  $V$  with invariant trace field  $k$  and invariant quaternion algebra  $B$ . Then the discriminant  $\text{disc}(B)$  of  $B$  satisfies  $|\text{disc}(B)| \leq [10^{93}V^{13}]^{10}$  (respectively,  $|\text{disc}(B)| \leq 10^{57}V^7$ ).*

*Proof.* We establish the lemma for 3–manifolds as the case of hyperbolic surfaces is similar. Towards that goal, set  $V'$  to be the covolume of a minimal covolume maximal arithmetic subgroup in the commensurability class associated to  $B$  and  $k$ . It is known by work of Chinburg–Friedman[20, pp. 8] that

$$(17) \quad V' = \frac{2\pi^2 \zeta_k(2) d_k^{\frac{3}{2}} \Phi(\text{disc}(B))}{(4\pi^2)^{n_k} [k_B : k]},$$

where

$$\Phi(\text{disc}(B)) = \prod_{p|\text{disc}(B)} \left( \frac{|p| - 1}{2} \right)$$

and  $k_B$  is the maximal abelian extension of  $k$  which has 2–elementary Galois group, is unramified at all finite primes of  $k$  and in which all (finite) prime divisors of  $\text{disc}(B)$  split completely. It is clear that  $k_B$  is contained in the strict class field of  $k$ , hence

$$[k_B : k] \leq 2^{r_1(k)} h_k = 2^{n_k - 2} h_k.$$

Let  $\omega_2(B)$  denote the number of prime divisors of  $\text{disc}(B)$  which have norm 2. From the Euler product expansion of  $\zeta_k(s)$ , we deduce that  $\zeta_k(2) \geq (\frac{4}{3})^{\omega_2(B)}$ . In combination with (17), we conclude that

$$(18) \quad V' \geq \frac{(\frac{4}{3})^{\omega_2(B)} d_k^{\frac{3}{2}} |\text{disc}(B)|}{(4\pi^2)^{n_k} 4^{\omega_2(B)} 2^{n_k - 2} h_k} \geq \frac{d_k^{\frac{3}{2}} |\text{disc}(B)|}{(8\pi^2)^{n_k} 3^{\omega_2(B)} h_k}.$$

Now, we have the trivial bound  $\omega_2(B) \leq n_k$  and the inequality

$$h_k \leq 242 d_k^{\frac{3}{4}}$$

found in [58, Lemma 3.1]. Coupling these two inequalities with (18) produces

$$(19) \quad V' \geq \frac{d_k^{\frac{3}{2}} |\text{disc}(B)|}{242(24\pi^2)^{n_k} d_k^{\frac{3}{4}}} \geq \frac{|\text{disc}(B)|}{242(24\pi^2)^{n_k}}.$$

Our proof is now complete upon applying Chinburg–Friedman [18, Lemma 4.3], which implies that  $n_k \leq 23 + \log(V')$ , to (19) in tandem with the fact that  $V \geq V'$ .  $\square$

We now prove Corollary 1.8.

*Proof of Corollary 1.8.* Let  $k$  be a totally real number field and  $B$  be a quaternion division algebra over  $k$  which is ramified at all but one real places of  $k$ . If  $\rho : B \rightarrow M(2, \mathbf{R})$  is a representation and  $\mathcal{O}$  is an order of  $B$ , then it is easy to see that the invariant trace field of  $\Gamma_{\mathcal{O}}$  is  $k$ ; recall that  $\Gamma_{\mathcal{O}}$  is defined to be  $P\rho(\mathcal{O}^1)$ . It is similarly clear that the invariant quaternion algebra of  $\Gamma_{\mathcal{O}}$  is  $B$ . Namely, since this algebra is a quaternion algebra over  $k$  that is visibly contained in  $B$ , the asserted isomorphism follows from comparing dimensions. By definition, a Fuchsian group is arithmetic if it is commensurable with a group of the form  $\Gamma_{\mathcal{O}}$ , hence by Lemma 4.1 and the preceding discussion, to prove Corollary 1.8 it suffices to bound the number of quaternion division algebras  $B$  over  $k$  which are ramified at all real places of  $k$  and satisfy  $|\text{disc}(B)| \leq [10^{93} V^{13}]^{10}$ . The corollary now follows from Theorem 1.5.  $\square$

The proof of Corollary 1.9 is similar and is left to the reader.

**4.2. Lengths of geodesics arising from quadratic extensions.** We begin this subsection with a result that will permit us to work with Kleinian groups derived from a quaternion algebra.

**Proposition 4.2.** *Let  $\Gamma$  be a Kleinian group with finite covolume  $V$  and let  $\Gamma^{(2)}$  be the subgroup of  $\Gamma$  generated by squares. Then there exists an absolute, effectively computable constant  $C$  such that the covolume of  $\Gamma^{(2)}$  is at most  $e^{CV}$ .*

*Proof.* It is well-known that because  $\Gamma$  has finite covolume it is finitely generated. Let  $d(\Gamma)$  denote the minimal number of generators of  $\Gamma$ . By Theorem 2.6, there exists an absolute constant  $C$  such that  $d(\Gamma) < C_0 V$ . It is now clear that  $\Gamma/\Gamma^{(2)}$  is a finite elementary abelian 2-group of order at most  $2^{d(\Gamma)}$ . As the covolume of  $\Gamma^{(2)}$  is  $[\Gamma : \Gamma^{(2)}] \cdot V$ , the result follows.  $\square$

**Lemma 4.3.** *Let  $\Gamma'$  be an arithmetic Kleinian group or arithmetic Fuchsian group derived from a quaternion algebra  $B$  over a number field  $k$  which has covolume  $V'$  and is contained in  $\Gamma_{\mathcal{O}}$ , where  $\mathcal{O}$  is a maximal order of  $B$ . Then  $[\Gamma_{\mathcal{O}} : \Gamma'] \leq V'$ .*

*Proof.* We will prove the lemma in the case that  $\Gamma'$  is an arithmetic Kleinian group. The proof of the Fuchsian case is virtually identical and left to the reader. The work of Borel [7] (see also [65, Chapter 11]) shows that the covolume  $V_{\mathcal{O}}$  of  $\Gamma_{\mathcal{O}}$  is equal to

$$(20) \quad \frac{d_k^{3/2} \zeta_k(2) \prod_{\mathfrak{p}|\text{disc}(B)} (|\mathfrak{p}| - 1)}{(4\pi^2)^{n_k-1}}.$$

As  $V_{\mathcal{O}} \cdot [\Gamma_{\mathcal{O}} : \Gamma'] = V'$  we see that

$$(21) \quad [\Gamma_{\mathcal{O}} : \Gamma'] = \frac{V'(4\pi^2)^{n_k-1}}{d_k^{3/2} \zeta_k(2) \prod_{\mathfrak{p}|\text{disc}(B)} (|\mathfrak{p}| - 1)}$$

$$(22) \quad \leq \frac{V'(4\pi^2)^{n_k-1}}{d_k^{3/2}}.$$

The discriminant bounds of Odlyzko [75] and Poitou [79] (see also [12, Theorem 2.4]) show that  $\log(d_k) \geq 4r_1 + 6r_2$  where  $r_1$  is the number of real places of  $k$  and  $r_2$  is the number of complex places of  $k$ . It is well-known that in our situation it must be the case that  $k$  has a unique complex place, hence  $r_1 = n_k - 2$  and  $r_2 = 1$ . We conclude that  $d_k^{3/2} \geq e^{6(n_k-2)} e^9$ . Applying this bound to equation (22) and simplifying finishes the proof.  $\square$

**Remark.** It is implicit in the statement of Lemma 4.3 and in any event follows from the ideas of the lemma's proof that if  $\mathcal{O}$  is a maximal order of  $B$  then  $\Gamma_{\mathcal{O}}$  has covolume at least 1.

We next need a simple lemma that provides a bound for the regulator of a maximal subfield.

**Lemma 4.4.** *Let  $k$  be a number field with a unique complex place,  $B$  a quaternion algebra over  $k$  which is ramified at all real places of  $k$  and  $L$  a maximal subfield of  $B$ . Then the regulator  $\text{Reg}_L$  of  $L$  satisfies  $\text{Reg}_L \leq d_L^{n_k}$ .*

*Proof.* Let  $r_1(L)$  (respectively  $r_2(L)$ ) denote the number of real (respectively complex) places of  $L$ . Since  $L$  embeds into  $B$ , the Albert–Brauer–Hasse–Noether theorem implies that  $r_1(L) = 0$  and  $r_2(L) = n_k$ . The class number formula [54, pp. 300] implies that

$$\text{Reg}_L = \frac{\omega_L d_L^{\frac{1}{2}} \kappa_L}{(2\pi)^{n_k} h_L},$$

where  $\omega_L$  is the number of roots of unity lying in  $L$ ,  $\kappa_L$  is the residue at  $s = 1$  of the Dedekind zeta function  $\zeta_L(s)$  and  $h_L$  is the class number of  $L$ . As  $h_L \geq 1$ ,  $\omega_L \leq 2n_L^2 = 8n_k^2$  and  $8n^2 \leq (2\pi)^n$  for all  $n \geq 2$ , we see that

$$\text{Reg}_L \leq d_L^{\frac{1}{2}} \kappa_L \leq d_L^{\frac{1}{2}} \log(d_L^{\frac{1}{2}})^{n_L-1} \leq d_L^{\frac{1}{2}} d_L^{n_k-\frac{1}{2}} = d_L^{n_k},$$

where the second inequality follows from [59, Proposition 2].  $\square$

We will also need the following analog of Lemma 4.4, whose proof is virtually identical to that of Lemma 4.4.

**Lemma 4.5.** *Let  $k$  be a totally real number field,  $B$  a quaternion algebra over  $k$  which is ramified at all but one real places of  $k$  and  $L$  a maximal subfield of  $B$  which is not totally complex. Then the regulator  $\text{Reg}_L$  of  $L$  satisfies  $\text{Reg}_L \leq d_L^{n_k}$ .*

Before continuing further, we briefly survey some basic results about logarithmic heights of algebraic numbers. For a number field  $k$  and  $\mathfrak{p} \in \mathcal{P}_k$ , we normalize the associated valuation  $|\cdot|_{\mathfrak{p}}$  in the usual way so that for each  $\alpha$  in  $k$ , we have

$$\prod_{\mathfrak{p}|\infty} |\alpha|_{\mathfrak{p}} = |\text{Norm}_{k/\mathbf{Q}}(\alpha)|$$

and

$$\prod_{\mathfrak{p} \in \mathcal{P}_k} |\alpha|_{\mathfrak{p}} = 1.$$

We define the **logarithmic height of  $\alpha$  relative to  $k$**  to be

$$h_k(\alpha) = \sum_{\mathfrak{p} \in \mathcal{P}_k} \log \left( \max \left\{ 1, |\alpha|_{\mathfrak{p}} \right\} \right).$$

The **absolute height of  $\alpha$**  is

$$H(\alpha) = [k : \mathbf{Q}]^{-1} h_k(\alpha)$$

and is independent of the field  $k$ , and the **height of  $\alpha$  relative to  $\mathbf{Q}(\alpha)$**  is the logarithm of the Mahler measure of the minimal polynomial of  $\alpha$ . The proof of the following lemma is straightforward.

**Lemma 4.6.** *Let the notation be as above.*

- (i) *For all nonzero  $n \in \mathbf{Z}$ ,  $H(\alpha^n) = |n| \cdot H(\alpha)$ .*
- (ii) *For all algebraic numbers  $\beta$ ,  $H(\alpha\beta) \leq H(\alpha) + H(\beta)$ .*
- (iii) *If  $\alpha$  and  $\beta$  are Galois conjugates then  $H(\alpha) = H(\beta)$ .*

**Proposition 4.7.** *Let  $k$  be a number field which is either totally real or else has a unique complex place and let  $B$  be a quaternion division algebra defined over  $k$  in which all but one real places of  $k$  ramify if  $k$  is totally real and in which all real places of  $k$  ramify otherwise. Let  $\Gamma$  be an arithmetic Fuchsian or Kleinian group which has covolume  $V$ , invariant trace field  $k$  and invariant quaternion algebra  $B$ . Let  $L/k$  be a quadratic field extension which embeds into  $B$  and suppose further that  $L$  is not totally complex if  $k$  is totally real. Then there exist absolute, effectively computable constants  $C_1, C_2$  such that  $L = k_{\gamma}$  for some hyperbolic element  $\gamma \in \Gamma$  with  $\ell(\gamma) \leq e^{C_1 V} d_L^{C_2 + \log(V)}$ .*

*Proof.* We prove the proposition in the case that  $k$  has a unique complex place. The case in which  $k$  is totally real has an identical proof.

As every real place of  $k$  is ramified in  $B$ , we see that  $L$  embeds into  $B$  implies, by the Albert–Brauer–Hasse–Noether theorem, that  $L$  is totally complex. It now follows from Dirichlet’s unit theorem that the  $\mathbf{Z}$ –rank of  $\mathcal{O}_L^*$  is strictly greater than that of  $\mathcal{O}_k^*$ . From this we conclude that every system of fundamental units of  $\mathcal{O}_L^*$  contains a fundamental unit  $u_0 \in \mathcal{O}_L^*$  such that  $u_0^n \notin k$  for any  $n \geq 1$ . Consequently, we must have that  $L = k(u^n)$  for all  $n \neq 0$ . Let  $\sigma$  denote the non-trivial automorphism of  $\text{Gal}(L/k)$  and define  $u = u_0/\sigma(u_0)$ . It is clear that  $\text{Norm}_{L/k}(u) = 1$  and that  $u^n \notin \mathcal{O}_k^*$  for any  $n \geq 1$ . By [11] (see also [48]) we may take  $u_0$  to have logarithmic height (relative to  $L$ )

$$h_L(u_0) \leq n_k^{11n_k} \text{Reg}_L.$$

It follows from Lemma 4.6 that

$$h_L(u) \leq 2n_k^{11n_k} \text{Reg}_L,$$

and since  $[L : \mathbf{Q}] = 2n_k$  we see as well that

$$H(u) \leq n_k^{11n_k-1} \text{Reg}_L.$$

As  $\Gamma^{(2)}$  is derived from the quaternion algebra  $B$  [65, Chapter 3], there exists a maximal order  $\mathcal{O}$  of  $B$  such that  $\Gamma^{(2)} \subset \Gamma_{\mathcal{O}}^1$ . Recall,  $k_B$  is the maximal abelian extension of  $k$  of exponent 2 in which all prime divisors of  $\text{disc}(B)$  split completely. We now have two cases to consider.

Suppose first that  $L \not\subset k_B$ . Then every maximal order of  $B$  admits an embedding of  $\mathcal{O}_k[u]$  ([19, Theorem 3.3]; see also [57, Proposition 5.4]), hence we may assume that  $u \in \mathcal{O}$ . Let  $\gamma'$  be the image in  $\Gamma_{\mathcal{O}}^1$  of  $u$ . Proposition 4.2 and Lemma 4.3 show that  $\gamma = \gamma'^n \in \Gamma^{(2)} \subset \Gamma$  for some  $n \leq e^{C_0 V}$  and constant  $C_0$ . Moreover, Lemma 4.6 implies that

$$H(\gamma) \leq e^{C_0 V} n_k^{11n_k-1} \text{Reg}_L.$$

As the logarithm of the Mahler measure of the minimal polynomial of  $\gamma$  is less than  $2n_k H(\gamma)$ , we deduce, by [65, Lemma 12.3.3], that

$$\ell(\gamma) \leq 4e^{C_0 V} n_k^{11n_k} \text{Reg}_L.$$

By Lemma 4.4,

$$\ell(\gamma) \leq 4e^{C_0 V} n_k^{11n_k} d_L^{n_k}.$$

Lemma 4.3 of [18] shows that  $n_k \leq 23 + \log(V)$ , hence there exist a constant  $C_1$  such that

$$\ell(\gamma) \leq e^{C_1 V} d_L^{23+\log(V)}.$$

Suppose now that  $L \subset k_B$  and let  $\mathcal{E}$  be a maximal order of  $B$  which contains  $u$ . By Proposition 2.3 there exists an absolute constant  $C_2 > 0$  and an integer  $n \leq d_L^{C_2}$  such that  $u^n \in \mathcal{O}^1$ . The arguments of the previous paragraph show that there exists  $\gamma \in \Gamma^{(2)} \subset \Gamma$  such that

$$\ell(\gamma) \leq e^{C_1 V} d_L^{C_2+\log(V)},$$

finishing our proof. □

**Remark.** Proposition 4.7 is an effective version of Theorem 12.2.6 of [65].

**4.3. Corollary 1.10: Counting non-commensurable geodesics.** We begin with a definition. Let  $\Gamma$  be an arithmetic Fuchsian or Kleinian group and  $\gamma_1, \gamma_2 \in \Gamma$  be hyperbolic elements with associated closed geodesics lengths  $\ell(\gamma_1), \ell(\gamma_2)$ . We say that these geodesics are **rationally inequivalent** if  $\ell(\gamma_1)$  and  $\ell(\gamma_2)$  are not rational multiples of one another.

**Theorem 4.8.** *Let  $k$  be a number field of degree  $n_k$ , discriminant  $d_k$  that is totally real (has a unique complex place, respectively). Let  $B$  be a quaternion algebra over  $k$  which is ramified at all but one real places of  $k$  (respectively, at all real places of  $k$ ) and let  $\mathcal{O}$  be a maximal order of  $B$ . Then for all sufficiently large  $x$ , the orbifold  $\mathbf{H}^2/\Gamma_{\mathcal{O}}$  (respectively,  $\mathbf{H}^3/\Gamma_{\mathcal{O}}$ ) contains at least*

$$\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$$

*rationally inequivalent closed geodesics of length at most*

$$\left[ 2n_k^{11n_k-1} d_k^{2n_k} \right] x^{n_k}.$$

*Proof.* By Theorem 1.6 and the well-known fact that  $\zeta_k(s) \leq \zeta(s)^{n_k}$ , for all sufficiently large real  $x > 0$  there are at least

$$\left[ 2\kappa_k \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$$

quadratic extensions  $L/k$  which embed into  $B$  and satisfy  $|\Delta_{L/k}| < x$ . When  $k$  is totally real, if an extension  $L/k$  embeds into  $B$  then  $L$  is either totally complex or else has 2 real places and  $n_k - 2$  complex places. Combining Theorem 1.6 with Proposition 3.3(iii) now shows that when  $k$  is totally real there are at least

$$\left[ \kappa_k \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$$

quadratic extensions  $L/k$  which embed into  $B$ , satisfy  $|\Delta_{L/k}| < x$ , and are not totally complex.

The proof of Proposition 4.7 shows that with at most finitely many exceptions, the extensions described above are all of the form  $L = k\gamma$ , where  $\gamma$  is a hyperbolic element in  $\Gamma_{\mathcal{O}}$  having length

$$\ell(\gamma) \leq 2n_k^{11n_k-1} \text{Reg}_L.$$

Lemma 6.3 of [21] shows that if  $\lambda_1, \lambda_2$  are eigenvalues of hyperbolic elements  $\gamma_1, \gamma_2 \in \Gamma_{\mathcal{O}}$  whose lengths are rationally equivalent then either  $k(\lambda_1) = k(\lambda_2)$  or  $k(\lambda_1) = k(\overline{\lambda_2})$ . It follows that for  $x$  sufficiently large, at least

$$\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$$

of the geodesics associated to the hyperbolic elements  $\gamma$  referred to in the previous paragraph are rationally inequivalent. The theorem now follows from Lemma 4.4 and the formula  $d_L = |\Delta_{L/k}| d_k^2$ .  $\square$

Every arithmetic Kleinian group in the commensurability class defined by the number field  $k$  and quaternion algebra  $B$  is commensurable with  $\Gamma_{\mathcal{O}}$ , allowing us to deduce Corollary 1.10.

*Proof of Corollary 1.10.* Let  $\Gamma^{(2)}$  be the subgroup of  $\Gamma$  generated by squares. By Proposition 4.2 (which follows trivially from the Gauss–Bonnet formula when  $\Gamma$  is a Fuchsian group) the covolume of  $\Gamma^{(2)}$  is at most  $e^{CV}$  for some absolute, effectively computable constant  $C$ . It is well-known [65, Corollary 8.3.5] that there

is a maximal order  $\mathcal{O}$  of  $B$  such that  $\Gamma^{(2)} \leq \Gamma_{\mathcal{O}}$ , and it was shown in Lemma 4.3 that the index of  $\Gamma^{(2)}$  in  $\Gamma_{\mathcal{O}}$  is at most  $e^{CV}$ . It follows immediately from Theorem 4.8 that for  $x$  sufficiently large, the orbifold  $\mathbf{H}^3/\Gamma$  contains at least

$$\left\lceil \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} \right\rceil x$$

rationally inequivalent closed geodesics of length at most

$$e^{CV} (2n_k^{11n_k-1} d_k^{2n_k}) x^{n_k}.$$

The corollary now follows from the inequality  $n_k \leq 23 + \log(V)$  [18, Lemma 4.3], from the inequality  $d_k \leq V^{22}$  [58, proof of Theorem 4.1], and from elementary logarithm inequalities.  $\square$

**4.4. Counting manifolds with prescribed geodesic lengths.** Let  $M$  be an arithmetic hyperbolic 2-orbifold (3-orbifold) which contains closed geodesics of lengths  $\ell_1, \dots, \ell_N$ . For a real number  $V > 0$ , let  $N_{\ell_1, \dots, \ell_N}^2(V)$  (respectively,  $N_{\ell_1, \dots, \ell_N}^3(V)$ ) denote the maximum cardinality of a family of arithmetic, pairwise non-commensurable, hyperbolic 2-orbifolds (respectively, 3-orbifolds) all of whose members have closed geodesics of lengths  $\ell_1, \dots, \ell_N$  and volume at most  $V$ . It is a result of Borel and Prasad [9] that there are at most finitely many arithmetic hyperbolic 2- or 3-orbifolds with volume at most  $V$ , hence  $N_{\ell_1, \dots, \ell_N}^2(V)$  and  $N_{\ell_1, \dots, \ell_N}^3(V)$  are well-defined. As an application to Theorem 1.7 we provide upper and lower bounds for these functions.

Before stating these bounds however, we require some further notation which we will use for the remainder of this section. We set  $\Gamma$  to be the orbifold fundamental group of  $M$ . With  $\ell_1, \dots, \ell_N$  as above, let  $\gamma_i$  denote a hyperbolic element of  $\Gamma$  with associated geodesic of length  $\ell_i$ . Furthermore, let  $\lambda_i$  denote the eigenvalue of a pre-image of  $\gamma_i$  in  $\mathrm{SL}(2, \mathbf{C})$  satisfying  $|\lambda_i| > 1$ .

We now state our bounds for  $N_{\ell_1, \dots, \ell_N}^2(V)$  and  $N_{\ell_1, \dots, \ell_N}^3(V)$ . Below, Theorem 4.9 deals with the case in which  $\{\lambda_1, \dots, \lambda_N\} \not\subset \mathbf{R}$  and Theorem 4.10 deals with the case in which  $\{\lambda_1, \dots, \lambda_N\} \subset \mathbf{R}$ .

**Theorem 4.9.** *Let  $M$  be an arithmetic hyperbolic 3-manifold which is derived from a quaternion algebra and contains closed geodesics of lengths  $\ell_1, \dots, \ell_N$ . If there is an  $i$  such that  $\lambda_i$  is not real then exactly one of the following are true:*

- (i) *There are only finitely many quaternion algebras defined over the invariant trace field  $k$  of  $\Gamma$  which are ramified at all real places of  $k$  and admit embeddings of  $k(\lambda_i)$  for all  $i$ . In this case there are positive real numbers  $c$  and  $V_0$  such that  $N_{\ell_1, \dots, \ell_N}^3(V) = c$  for all  $V > V_0$ .*
- (ii) *There are infinitely many commensurability classes of hyperbolic 3-manifolds containing orbifolds with closed geodesics of lengths  $\ell_1, \dots, \ell_N$ . In this case there exist integers  $1 \leq r, s \leq N$  such that*

$$V / \log(V)^{1 - \frac{1}{2s}} \ll_M N_{\ell_1, \dots, \ell_N}^3(V) \ll_M V / \log(V)^{1 - \frac{1}{2r}}.$$

**Remark.** Let  $k^+$  denote the maximal totally real subfield of  $k$ . We remark that Lemma 2.3 of [21] shows that if  $k$  is not a quadratic extension of  $k^+$  then  $\Gamma$  will have no hyperbolic elements with real eigenvalue. In this situation the hypotheses of Theorem 4.9 will always be satisfied.

The techniques used to prove Theorem 4.9 can be applied, in much the same manner, to prove the following result.



**Theorem 4.10.** *Let  $M$  be an arithmetic hyperbolic 2–manifold (3–manifold) which is derived from a quaternion algebra and contains closed geodesics of lengths  $\ell_1, \dots, \ell_N$ . If  $\lambda_i$  is real for all  $i$  then exactly one of the following are true:*

- (i) *There are only finitely many quaternion algebras defined over the invariant trace field  $k$  of  $\Gamma$  which are ramified at all but one real places of  $k$  (respectively, at all real places of  $k$ ) and admit embeddings of  $k(\lambda_i)$  for all  $i$ .*
- (ii) *There are infinitely many commensurability classes of hyperbolic 2–manifolds (respectively, 3–manifolds) containing orbifolds with closed geodesics of lengths  $\ell_1, \dots, \ell_N$  and invariant trace field  $k$ . In this case there exist integers  $1 \leq r, s, t \leq N$  such that*

$$V / \log(V)^{1-\frac{1}{2^r}} \gg_M N_{\ell_1, \dots, \ell_N}^2(V) \gg_M V / \log(V)^{1-\frac{1}{2^s}}$$

$$(\text{respectively, } N_{\ell_1, \dots, \ell_N}^3(V) \gg_M V / \log(V)^{1-\frac{1}{2^t}}).$$

Note that Theorems 4.9 and 4.10 both deal with geodesics on arithmetic hyperbolic 2– and 3–manifolds which are derived from quaternion algebras, as opposed to arbitrary arithmetic hyperbolic 2– and 3–manifolds. The reason for this restriction amounts to the following observation (which will be made more precise and proven as part of the proof of Theorem 4.9). Let  $M$  be as in Theorem 4.9. The commensurability classes of arithmetic hyperbolic 3–manifolds containing orbifolds with closed geodesics of lengths  $\ell_1, \dots, \ell_N$  are in one-to-one correspondence with quaternion algebras over  $k$  which ramify at all real places of  $k$  and admit embeddings of  $k(\lambda_1), \dots, k(\lambda_N)$ . This correspondence breaks down however, when the manifold  $M$  is arithmetic but not necessarily derived from a quaternion algebra. In this more general setting however, we are able to prove the following.

**Theorem 4.11.** *Let  $M$  be an arithmetic hyperbolic 2–manifold (3–manifold, respectively) which contains closed geodesics of lengths  $\ell_1, \dots, \ell_N$ . If there are infinitely many primes of  $k$  which do not split in any of the extensions  $k(\lambda_i)/k$  then there are infinitely many commensurability classes of hyperbolic surfaces (respectively, 3–manifolds) containing orbifolds with closed geodesics of lengths  $\ell_1, \dots, \ell_N$ .*

**Remark.** If there are only finitely many primes of  $k$  which do not split in any of the extensions  $k(\lambda_i)/k$  then there are at most finitely many commensurability classes of hyperbolic 2– or 3–manifolds containing orbifolds with closed geodesics of lengths  $\ell_1, \dots, \ell_N$  and having invariant trace field  $k$ . In many situations however (for instance if  $M$  is a 2– or 3–manifold such that  $\{\lambda_1, \dots, \lambda_N\} \not\subset \mathbf{R}$ ), any arithmetic hyperbolic 2– or 3–orbifold containing closed geodesics of lengths  $\ell_1, \dots, \ell_N$  must have invariant trace field  $k$ . See for instance Proposition 4.13 and [21, Lemma 2.3]. In these situations the hypothesis in Theorem 4.11 is both necessary and sufficient.

4.4.1. *Proof of Theorem 4.9.* We begin with a proposition that will be needed in the proof of Theorem 4.9.

**Proposition 4.12.** *Let  $B$  be a quaternion algebra over  $k$  which admits embeddings of  $k(\lambda_1), \dots, k(\lambda_N)$  and  $\mathcal{O}$  be a maximal order of  $B$ . If a finite prime of  $k$  ramifies in  $B$  then the orbifold associated to  $\Gamma_{\mathcal{O}}$  contains closed geodesics of lengths  $\ell_1, \dots, \ell_N$ .*

*Proof.* For each  $i = 1, \dots, N$ , fix a quadratic  $\mathcal{O}_k$ –order  $\Omega_i \subset k(\lambda_i)$  which contains a pre-image in  $k(\lambda_i)$  of  $\gamma_i$ . Because of our assumption that  $B$  ramifies at a finite prime of  $k$ , a theorem of Chinburg and Friedman [19, Theorem 3.3] implies that every maximal order of  $B$ , in particular  $\mathcal{O}$ , contains a conjugate of all of

the quadratic orders  $\Omega_i$ . The proposition now follows from the fact that the length of the closed geodesic associated to  $\gamma_i$  coincides with the length of the closed geodesic associated to any conjugate of  $\gamma_i$ .  $\square$

We now prove Theorem 4.9.

*Proof of Theorem 4.9.* Let  $k$  denote the invariant trace field of  $\Gamma$ ,  $B$  the invariant quaternion algebra of  $\Gamma$  and for  $i = 1, \dots, N$ , let  $L_i$  denote the quadratic extension  $k(\lambda_i)$  of  $k$ . By hypothesis there exists an  $i$  such that  $\lambda_i \notin \mathbf{R}$ . Lemma 2.3 of [21] shows that this implies that the image in  $\mathbf{C}$  of  $k$  is  $\mathbf{Q}(\mathrm{tr}(\gamma_i)) = \mathbf{Q}(\lambda_i + \lambda_i^{-1})$ . Throughout the remainder of this proof we will identify  $k$  with its image in  $\mathbf{C}$ .

Suppose that  $\Gamma'$  is an arithmetic Kleinian group such that the quotient orbifold has closed geodesics of lengths  $\ell_1, \dots, \ell_N$ . Taking powers of the elements  $\gamma_i$  as needed, we may assume that  $\Gamma'$  is derived from a quaternion algebra. Let  $k'$  denote the invariant trace field of  $\Gamma'$  and  $B'$  the invariant quaternion algebra. The formula (3) shows that if  $\gamma'_i$  is an element of  $\Gamma'$  whose associated closed geodesic has length  $\ell_i$  then  $\mathrm{tr}(\gamma_i) = \mathrm{tr}(\gamma'_i)$  (up to sign). In particular this implies that up to complex conjugation we have  $k = \mathbf{Q}(\mathrm{tr}(\gamma_i)) = \mathbf{Q}(\mathrm{tr}(\gamma'_i)) = k'$ . We may therefore suppose that  $B'$  is defined over  $k$ . The results of [65, Chapter 12] now imply that  $B'$  admits embeddings of  $L_1, \dots, L_N$ . Conversely, suppose that  $B'$  is a quaternion algebra over  $k$  which satisfies the following two conditions:

- (i)  $B'$  is ramified at all real places and at at least one finite prime of  $k$ ,
- (ii)  $B'$  admits embeddings of  $L_1, \dots, L_N$ .

Proposition 4.12 then shows that if  $\mathcal{O}'$  is a maximal order of  $B'$  then  $\Gamma_{\mathcal{O}'}$  is an arithmetic Kleinian group whose quotient orbifold contains closed geodesics of lengths  $\ell_1, \dots, \ell_N$ . Putting these together, we see that  $N_{\ell_1, \dots, \ell_N}(V)$  is asymptotic to the number of isomorphism classes of quaternion algebras over  $k$  which are ramified at all real places of  $k$  and which admit embeddings of  $L_1, \dots, L_N$ . (Note that all but finitely many quaternion algebras over  $k$  ramify at a finite prime of  $k$ .) The first assertion is an immediate consequence of this.

In order to prove the second assertion we first show that

$$N_{\ell_1, \dots, \ell_N}^3(V) \ll_M V / \log(V)^{1-\frac{1}{2^r}}$$

for some  $1 \leq r \leq N$ . Suppose that  $\Gamma'$  is an arithmetic Kleinian group whose quotient orbifold has closed geodesics of lengths  $\ell_1, \dots, \ell_N$  and let  $V'$  denote the covolume of  $\Gamma'$ . If we let  $V_{\mathcal{C}}$  denote the volume of a minimal volume orbifold in the commensurability class  $\mathcal{C}$  of  $\Gamma$ , then of course we see that  $V' \geq V_{\mathcal{C}}$ . Borel's formula [7] for  $V_{\mathcal{C}}$  makes it clear that there exists a constant  $c$ , which depends on  $k$ , such that  $V_{\mathcal{C}} \geq c |\mathrm{disc}(B')|$  where  $B'$  is the invariant quaternion algebra of  $\Gamma'$  and  $|\mathrm{disc}(B')|$  the norm of its discriminant. It follows from the discussion above that  $B'$  is defined over  $k$  and it is clear that  $B'$  admits embeddings of  $L_1, \dots, L_N$ . As  $|\mathrm{disc}(B')| \leq cV'$ , we conclude that the number of commensurability classes of arithmetic hyperbolic 3-orbifolds containing an orbifold with closed geodesics of lengths  $\ell_1, \dots, \ell_N$  is at most a constant multiple of the number of quaternion algebras over  $k$  which admit embeddings of  $L_1, \dots, L_N$ . That  $N_{\ell_1, \dots, \ell_N}^3(V) \ll_M V^{1/2} / \log(V)^{1-\frac{1}{2^r}}$  for some  $1 \leq r \leq N$  now follows from Theorem 1.7.

The proof that  $N_{\ell_1, \dots, \ell_N}^3(V) \gg_M V / \log(V)^{1-\frac{1}{2^s}}$  for some  $1 \leq s \leq N$  follows from the same ideas that were used in the previous paragraph, though applied to orbifolds of the form considered in Proposition 4.12.  $\square$

4.4.2. *Remarks about the proof of Theorem 4.10.* The proof of Theorem 4.10 follows from the same arguments that were used to prove the analogous statements in Theorem 4.9, hence we omit it. We do, however, record the following proposition which serves as a substitute for Lemma 2.3 of [21] in the Fuchsian case.

**Proposition 4.13.** *Let  $\Gamma$  be an arithmetic Fuchsian group derived from a quaternion algebra  $B$  defined over a totally real field  $k$ . If  $\gamma \in \Gamma$  is a hyperbolic element with eigenvalue  $\lambda_\gamma$  then  $k = \mathbf{Q}(\mathrm{tr}(\gamma))$ .*

*Proof.* In essence this proposition follows from the analogous result for Kleinian groups [21, Lemma 2.3]. Let  $\Gamma_0$  be an arithmetic Kleinian group derived from a quaternion algebra which contains  $\Gamma$  and whose invariant trace field  $k_0$  is a quadratic extension of  $k$ . Note, the existence of such a group  $\Gamma_0$  follows from the results in [65, Chapter 9]. Set  $F = \mathbf{Q}(\mathrm{tr}(\gamma))$ . Since  $\gamma \in \Gamma_0$  and  $\lambda_\gamma \in \mathbf{R}$ , [21, Lemma 2.3] shows that  $[k_0 : F] = 2$  and that  $F$  is the maximal totally real subfield of  $k_0$ . It is now clear that  $F = k$ , completing the proof.  $\square$

We now make a few comments about why the techniques used to prove Theorem 4.9 do not suffice to prove an upper bound for  $N_{\ell_1, \dots, \ell_N}^3(V)$ .

Recall that the proof of the upper bound for  $N_{\ell_1, \dots, \ell_N}^3(V)$  in Theorem 4.9 relied upon the fact that any arithmetic hyperbolic 3-orbifold containing closed geodesics of lengths  $\ell_1, \dots, \ell_N$  necessarily has  $k$  as its invariant trace field, hence our proof followed from counting quaternion algebras defined over  $k$  admitting embeddings of  $k(\lambda_1), \dots, k(\lambda_N)$ . Whereas this is the case for arithmetic Fuchsian groups by Proposition 4.13, it is not necessarily the case for 3-orbifolds in the context of Theorem 4.10. Indeed, let  $k^+$  denote the maximal totally real subfield of  $k$  and assume that  $k$  is a quadratic extension of  $k^+$ . Lemma 2.3 of [21] shows that  $k = \mathbf{Q}(\mathrm{tr}(\gamma_i))$  if  $\lambda_i$  is not real and  $k^+ = \mathbf{Q}(\mathrm{tr}(\gamma_i))$  if  $\lambda_i$  is real. As a consequence the invariant trace field of an arithmetic hyperbolic 3-orbifold containing closed geodesics of lengths  $\ell_1, \dots, \ell_N$  is a quadratic extension of  $k^+$ . This does not imply, however, that this invariant trace field need be equal to  $k$ . In theory one could obtain an upper bound for  $N_{\ell_1, \dots, \ell_N}^3(V)$  by counting the number of quadratic extensions of  $k^+$  with norm of relative discriminant less than some bound and having a unique complex place and then multiplying this count by the number of quaternion algebras defined over each field. The former count, for instance, has been computed by Cohen, Diaz y Diaz and Olivier [23, Corollary 3.14]. The latter count is given by Theorem 1.7 and contains a constant which depends on the invariants of the particular quadratic extension of  $k^+$  chosen. Because of how complicated this constant is, it is not clear how one could bound it by invariants of only  $k^+$ , which would in turn have to be related to the volume of arithmetic hyperbolic 3-orbifolds.

4.4.3. *Proof of Theorem 4.11.* We prove the theorem in the case in which  $M$  is a 3-manifold. The surface case has a proof which is virtually identical and thus left to the reader. Let  $\Gamma$  be the fundamental group of  $M$  and  $B$  the associated invariant quaternion algebra. We may assume without loss of generality that  $\Gamma$  is a maximal arithmetic subgroup of  $B^\times/k^\times$  and hence is of the form  $\Gamma = \Gamma_{S, \mathcal{O}}$  (in the notation of Chinburg and Friedman [19, Section 4]), where  $S$  is a finite set of primes of  $k$  and  $\mathcal{O}$  is a maximal order of  $B$ . For  $i = 1, \dots, N$ , let  $\overline{\gamma}_i \in \Gamma_{S, \mathcal{O}}$  be a pre-image of  $\gamma_i$  in  $B^\times/k^\times$  and  $y_i \in k(\lambda_i)$  be a pre-image of  $\gamma_i$  in  $B^\times$ . In order to prove the existence of infinitely many pairwise non-commensurable arithmetic hyperbolic 3-orbifolds containing closed geodesics of lengths  $\ell_1, \dots, \ell_N$  we will first construct an infinite number of quaternion algebras  $B_j$  over  $k$  (each of which ramifies at all real places of  $k$ ) with the property that for every  $j$ , the finite part of  $\mathrm{disc}(B)$  is a proper divisor of the finite part of  $\mathrm{disc}(B_j)$ . We will then construct, for every  $j$ , a maximal arithmetic subgroup  $\Gamma_j$  of  $B_j^\times/k^\times$  such that  $\Gamma_j$  contains, for  $i = 1, \dots, N$ , an element with the

same trace and norm as  $\bar{y}_i$ . It will follow that the associated orbifold will have closed geodesics of lengths  $\ell_1, \dots, \ell_N$ .

Our construction of the algebras  $B_j$  is straightforward. Let  $p_1, p_2, \dots$  be an infinite sequence of primes of  $k$  which do not split in any of the extensions  $k(\lambda_i)/k$ . Pruning this sequence as needed, we may assume that none of the primes  $p_i$  lie in the finite set  $S$  of primes mentioned in the previous paragraph nor do they divide  $\text{disc}(B)$ . Consider the sequence of moduli

$$\text{disc}(B)p_1p_2, \text{disc}(B)p_1p_3, \text{disc}(B)p_1p_4, \dots$$

As  $\text{disc}(B)$  must have an even number of divisors, as do the discriminants of all quaternion algebras over number fields, each of these moduli has an even number of divisors. Hence, there exist quaternion algebras  $B_1, B_2, B_3, \dots$  having these as their discriminants. It is clear that these algebras are pairwise non-isomorphic. Also note that by the Albert–Brauer–Hasse–Noether theorem, the quadratic extension  $k(\lambda_i)/k$  will embed into  $B_j$  if and only if no prime which ramifies in  $B_j$  splits in  $k(\lambda_i)/k$ . Because the extension  $k(\lambda_i)/k$  embeds into  $B$  (as we saw above), none of the divisors of  $\text{disc}(B)$  split in any of the extensions  $k(\lambda_i)/k$ . Further, by hypothesis no prime in the sequence  $p_1, p_2, \dots$  splits in any of the extensions  $k(\lambda_i)/k$ . We conclude that all of the algebras  $B_j$  admit embeddings of all of the extensions  $k(\lambda_i)/k$ .

In order to construct the maximal arithmetic subgroups  $\Gamma_j$  of  $B_j^\times/k^\times$ , we will need to make use of the following theorem of Chinburg and Friedman [19, Theorem 4.4]:

**Theorem 4.14** (Chinburg–Friedman). *Let  $k$  be a number field and  $B$  be a quaternion algebra over  $k$  in which at least one archimedean place of  $k$  is unramified. Suppose that  $y \in B^\times$  and consider the maximal arithmetic subgroup  $\Gamma_{S, \mathcal{D}}$  of  $B^\times/k^\times$ . If a conjugate of the image  $\bar{y} \in B^\times/k^\times$  of  $y$  is contained in  $\Gamma_{S, \mathcal{D}}$  then the following three conditions hold:*

- (i)  $\text{disc}(y)/\text{Norm}(y) \in \mathcal{O}_k$ ,
- (ii) If a prime  $\mathfrak{p}$  appears to an odd power in the prime ideal factorization of  $n(y)$  (that is,  $y$  is odd at  $\mathfrak{p}$ ), then  $\mathfrak{p} \in S \cup \text{Ram}_f(B)$ ,
- (iii) For each  $\mathfrak{p} \in S$  at least one of the following four conditions hold:
  - (a)  $y \in k$ ;
  - (b)  $y$  is odd at  $\mathfrak{p}$ ;
  - (c)  $k(y) \otimes_k k_{\mathfrak{p}}$  is not a field;
  - (d)  $\mathfrak{p}$  divides  $\text{disc}(y)/\text{Norm}(y)$ .

Conversely, if conditions (1), (2) and (3) hold, then a conjugate of  $\bar{y}$  is contained in  $\Gamma_{S, \mathcal{D}}$  except possibly when the following three conditions hold:

- (iv)  $k(y) \subset B$  is a quadratic field extension of  $k$ .
- (v) The extension  $k(y)/k$  and the algebra  $B$  are both unramified at all finite primes of  $k$  and ramify at precisely the same (possibly empty) set of real places of  $k$ . Further, all primes  $\mathfrak{p} \in S$  split in  $k(y)/k$ .
- (vi) All primes  $\mathfrak{p}$  dividing  $\text{disc}(y)/\text{Norm}(y)$  split in  $k(y)/k$ .

Suppose now that (1)–(6) hold. In this case the  $S$ -types of maximal orders  $\mathcal{D}$  of  $B$  is even and the  $\mathcal{D}$  for which a conjugate  $\bar{y}$  belongs to  $\Gamma_{S, \mathcal{D}}$  comprise exactly half of the  $S$ -types.

We now return to the proof of Theorem 4.11. Fix an integer  $j \geq 1$  and consider the quaternion algebra  $B_j$  defined above. Let  $\mathcal{O}$  be a maximal order of  $B_j$  and consider the maximal arithmetic subgroup  $\Gamma_j = \Gamma_{S, \mathcal{O}}$  of  $B_j^\times / k^\times$ . As  $B_j$  admits embeddings of  $k(\lambda_i)/k$  for all  $i$ , we will abuse notation slightly and identify these extensions with their images in  $B_j$ . We therefore consider the elements  $y_i$  referred to above (in the context of the algebra  $B$ ) as being contained in  $B_j$ . Because the elements  $y_i$  were all contained in  $\Gamma_{S, \mathcal{O}} \subset B^\times / k^\times$ , we see by Theorem 4.14 (and because  $B_j$  ramifies at a finite prime of  $k$ , hence condition (5) of Theorem 4.14 is not satisfied, and  $\text{Ram}_f(B) \subset \text{Ram}_f(B_j)$ ) that conjugates of the  $\bar{y}_i$  lie in  $\Gamma_j \subset B_j^\times / k^\times$ . Theorem 4.11 follows.

## 5. THEOREM 1.1: EFFECTIVE LENGTH RIGIDITY

**5.1. A technical lemma.** Let  $k$  be a number field of degree  $n_k$  with integral basis  $\Omega = \{\omega_1, \dots, \omega_{n_k}\}$ . We endow  $\mathcal{O}_k$  with the  $T_2$ -norm by setting

$$T_2(x) = \sum_{\sigma: k \hookrightarrow \mathbb{C}} |\sigma(x)|^2.$$

An immediate consequence of the arithmetic-geometric mean inequality is that  $T_2(x) \geq n_k$  for all  $x \neq 0$ .

Finally, with notation as above define

$$B(\Omega) = \prod_{\sigma: k \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_k} |\sigma(\omega_i)|.$$

**Lemma 5.1.** *Let  $k$  be a number field of degree  $n_k \geq 2$ . Then  $B(\Omega) \leq 2^{n_k^3} d_k^{n_k}$ .*

*Proof.* The proof follows from the following inequalities:

$$\begin{aligned} B(\Omega) &= \prod_{\sigma: k \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_k} |\sigma(\omega_i)| \leq \prod_{\sigma: k \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_k} T_2(\omega_i) \leq \prod_{\sigma: k \hookrightarrow \mathbb{C}} \prod_{i=1}^{n_k} T_2(\omega_i) \\ &\leq \prod_{\sigma: k \hookrightarrow \mathbb{C}} \left( 2^{n_k^2} d_k \right) \leq 2^{n_k^3} d_k^{n_k}, \end{aligned}$$

where the second to last inequality follows from Theorem 3 of [77]. □

## 5.2. Geodesics of bounded length arising from maximal subfields.

**Proposition 5.2.** *Let  $k$  be a number field of degree  $n_k$  which has a unique complex place,  $B$  be a quaternion division algebra defined over  $k$  in which all real places of  $k$  ramify and  $\Gamma$  be an arithmetic Kleinian group which has covolume  $V$ , invariant trace field  $k$ , and invariant quaternion algebra  $B$ . Then there exists a hyperbolic element  $\gamma \in \Gamma$  with eigenvalue  $\lambda = \lambda_\gamma$  such that  $\lambda^n$  is not real for any  $n \geq 1$  and which satisfies*

$$\ell(\gamma) \leq K e^{(\log(V) \log(V))}$$

for some absolute constant  $K$ .

*Proof.* In order to prove Proposition 5.2, we will make effective an argument of Chinburg, Hamilton, Long and Reid [21, pp. 10]. Let  $k^+$  denote the maximal totally real subfield of  $k$ . If  $k$  is not a quadratic extension of  $k^+$  then [21, Lemma 2.3] implies that every hyperbolic element of  $\Gamma$  has a non-real eigenvalue, hence our proof follows from Proposition 4.7. We may therefore assume that  $k$  is a quadratic extension of  $k^+$ .

The Chebotarev density theorem implies that there are infinitely many rational primes  $p$  which split completely in  $k/\mathbf{Q}$  and do not divide  $|\text{disc}(B)|$ .

In order to obtain an upper bound we will apply the following modification of the effective Chebotarev density theorem [53], due to Wang [93, Theorem 2-C]:

**Theorem 5.3** (Wang). *Let  $L/K$  be a finite Galois extension of number fields of degree  $n$ ,  $S$  a finite set of primes of  $K$  and  $[\theta]$  a conjugacy class in  $\text{Gal}(L/K)$ . Then there is a prime ideal  $\mathfrak{p}$  of  $K$  such that*

- (i)  $\mathfrak{p}$  is unramified in  $L$  and is of degree 1 over  $\mathbf{Q}$ ;
- (ii)  $\mathfrak{p} \notin S$ ;
- (iii)  $\left(\frac{L/K}{\mathfrak{p}}\right) = [\theta]$ , and
- (iv)  $|\mathfrak{p}| \leq d_L^C (n \log(N_S))^2$ ,

where  $C$  is an absolute, effectively computable constant and  $N_S = \prod_{q \in S} |q|$ .

Whereas we would like to apply Theorem 5.3 to the extension  $k/\mathbf{Q}$ , we cannot because it may be the case that  $k/\mathbf{Q}$  is not Galois. Because of this issue we consider the Galois closure  $\widehat{k}$  of  $k$ . The extension  $\widehat{k}/\mathbf{Q}$  is by definition Galois, has degree at most  $n_k!$  and has the property that a prime  $p$  of  $\mathbf{Q}$  splits completely in (resp. ramifies in)  $k$  if and only  $p$  splits completely in (resp. ramifies in)  $\widehat{k}$ . Moreover, a result of Serre [87, Proposition 6] shows that

$$d_{\widehat{k}} \leq d_k^{n_k!-1} n_k!^{n_k!}.$$

Let  $p$  be a fixed rational prime which splits completely in  $k$  and does not lie below any prime ramifying in  $B$ . By Theorem 5.3 (applied with  $K = \mathbf{Q}$  and  $L = \widehat{k}$ ) and the remarks in the previous paragraph, we may assume that

$$p \leq \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^A \cdot [n_k! \log |\text{disc}(B)|]^2.$$

Let  $\mathfrak{q}^+$  be a fixed prime of  $k^+$  lying above  $\mathfrak{p}$  and  $\mathfrak{q}_1, \mathfrak{q}_2$  be distinct primes of  $k$  lying above  $\mathfrak{q}^+$ .

Let  $L/k$  be a quadratic extension which is ramified at every prime divisor of  $\text{disc}(B)$  and furthermore satisfies that  $\mathfrak{q}_1$  ramifies in  $L/k$  and  $\mathfrak{q}_2$  splits in  $L/k$ . Then there exist primes  $\mathfrak{q}'_1, \mathfrak{q}'_2, \mathfrak{q}'_3$  of  $L$  such that  $\mathfrak{q}_1 \mathcal{O}_L = (\mathfrak{q}'_1)^2$  and  $\mathfrak{q}_2 \mathcal{O}_L = \mathfrak{q}'_2 \mathfrak{q}'_3$ . By Proposition 4.7 there exist absolute, effectively computable constants  $C_1, C_2$  such that  $L = k(\lambda(\gamma))$  for some hyperbolic element  $\gamma \in \Gamma$  with  $\ell(\gamma) \leq e_{C_1 V} d_L^{C_2 + \log(V)}$ . As the primes  $\mathfrak{q}'_1$  and  $\mathfrak{q}'_2$  both lie above  $\mathfrak{q}^+$  and have different ramification degrees, we can infer that the extension  $L/k^+$  is not Galois, hence  $\lambda(\gamma)$  is not real by [21, Lemma 2.3]. As  $k(\lambda(\gamma)) = k(\lambda(\gamma)^n)$  for all  $n \geq 1$ , our assertion that no power of  $\lambda(\gamma)$  is real follows from an identical argument.

In light of the above it remains only to bound  $d_L$  in terms of  $V$  and put all of our estimates together.

By Wang's effective version of the Grunwald–Wang theorem [93, Theorem 4-A] we may assume that the conductor  $\mathfrak{f}_{L/k}$  of the extension  $L/k$  satisfies

$$\begin{aligned} |\mathfrak{f}_{L/k}| &\leq 64^{n_k} B(\Omega_k) |\text{disc}(B)|^{2n_k} \cdot \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^{2A} \cdot [n_k! \log |\text{disc}(B)|]^4 \\ &\leq 64^{n_k} 2^{n_k^3} d_k^{n_k} |\text{disc}(B)|^{2n_k} \cdot \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^{2A} \cdot [n_k! \log |\text{disc}(B)|]^4, \end{aligned}$$



where the latter inequality follows from Lemma 5.1. The conductor-discriminant formula and the fact that  $d_L = |\Delta_{L/k}| d_k^2$  implies that

$$d_L \leq 64^{n_k} 2^{n_k^3} d_k^{n_k+2} |\text{disc}(B)|^{2n_k} \cdot \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^{2A} \cdot [n_k! \log |\text{disc}(B)|]^4.$$

It now follows that

$$\ell(\gamma) \leq e^{C_1 V} \left[ 64^{n_k} 2^{n_k^3} d_k^{n_k+2} |\text{disc}(B)|^{2n_k} \cdot \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^{2A} \cdot [n_k! \log |\text{disc}(B)|]^4 \right]^{C_2 + \log(V)}.$$

In order to bound this expression from above we will make use of the following three inequalities:

- (i)  $n_k \leq 23 + \log(V)$  (proven in [18, Lemma 4.3]),
- (ii)  $d_k \leq V^{22}$  (proven as a part of [58, Theorem 4.1]),
- (iii)  $|\text{disc}(B)| \leq 10^{57} V^7$  (proven in Lemma 4.1).

Substituting in these upper bounds, an elementary computation shows that  $\ell(\gamma) \leq C e^{(\log(V) \log(V))}$  for some absolute constant  $C$ . We use here that the term  $n_k!^{n_k!}$  essentially dominates over all of the others and that its size can be estimated using Stirling's formula. The proposition follows.  $\square$

**5.3. Theorem 1.3: Recognizing quaternion algebras via maximal subfields.** We begin by proving a lemma which will be needed in the proof of this subsection's main result.

**Lemma 5.4.** *For all  $x > 2$  we have*

$$\prod_{p \leq x} p \leq e^{\frac{21x}{\log^3(x)} + x}.$$

*Proof.* Let

$$P(x) = \prod_{p \leq x} p$$

so that  $\log(P(x))$  is the usual Chebyshev theta function. The lemma now follows from [32, Theorem 5.2].  $\square$

We now prove Theorem 1.3 from the introduction.

*Proof of Theorem 1.3.* Suppose that  $B \not\cong B'$ . Interchanging  $B$  and  $B'$  if necessary, we may assume that there exists a prime  $\mathfrak{p}$  of  $k$  (which may be either finite or real) which ramifies in  $B$  but not in  $B'$ . By hypothesis if  $\mathfrak{p}$  is not real archimedean then  $|\mathfrak{p}| < x$ . Let  $L/k$  be a quadratic field extension such that:

- (i)  $[L_{\mathfrak{q}} : k_{\mathfrak{q}}] = 2$  for all primes  $\mathfrak{q}$  of  $k$  with  $|\mathfrak{q}| < x$ ,  $\mathfrak{q} \neq \mathfrak{p}$  and all primes  $\mathfrak{q}$  of  $L$  lying above  $\mathfrak{q}$ ;
- (ii)  $[L_{\mathfrak{p}} : k_{\mathfrak{p}}] = 1$  for all primes  $\mathfrak{p}$  of  $L$  lying above  $\mathfrak{p}$ ; and
- (iii) all real places of  $k$  not equal to  $\mathfrak{p}$  ramify in  $L/k$ .

The existence of such an extension  $L/k$  follows from the Grunwald–Wang theorem. By employing Wang's effective version of the Grunwald–Wang theorem [93, Chapter 4] we can in fact find such an extension  $L/k$



whose conductor  $\mathfrak{f}_{L/k}$  satisfies

$$(23) \quad |\mathfrak{f}_{L/k}| \leq (32)^{n_k^2} B(\Omega) \left( \prod_{p \leq x} p \right)^{2n_k}.$$

Lemmas 5.1, 5.4, and the conductor-discriminant formula imply that the relative discriminant  $\Delta_{L/k}$  has norm less than the bound given in the proposition's statement. The first assertion of the theorem now follows from the Albert–Brauer–Hasse–Noether theorem, which implies that  $B'$  admits an embedding of  $L/k$  whereas  $B$  does not. The second assertion follows from straightforward modifications of the ideas used to prove the first assertion.  $\square$

**5.4. Proof of Theorem 1.1.** In this subsection, we prove Theorem 1.1. We start with a proposition.

**Proposition 5.5.** *Suppose that  $\Gamma$  is an arithmetic Fuchsian or Kleinian group with covolume less than  $V$  and which arises from the quaternion algebra  $B$ . If  $L$  is a quadratic extension of  $k$  which is not totally complex if  $\Gamma$  is a Fuchsian group and which has norm of discriminant less than the bound in the statement of Theorem 1.3 (applied with  $X = 10^{930}V^{130}$  if  $\Gamma$  is a Fuchsian group and  $X = 10^{57}V^7$  if  $\Gamma$  is a Kleinian group), then there exists a hyperbolic element  $\gamma \in \Gamma$  and absolute, effectively computable constants  $c_1, c_2$  such that  $L = k(\lambda(\gamma))$  and  $\ell(\gamma) \leq c_1 e^{c_2 \log(V)V^\alpha}$ , where  $\alpha = 130$  if  $\Gamma$  is a Fuchsian group and is equal to 7 otherwise.*

*Proof.* Proposition 4.7 shows that there exists a hyperbolic element  $\gamma \in \Gamma$  such that  $L = k(\lambda_\gamma)$  and  $\ell(\gamma) \leq e^{C_1 V} d_L^{C_2 + \log(V)}$  for absolute, effectively computable constants  $C_1, C_2$ . The result now follows from our hypothesis about  $|\Delta_{L/k}|$ , the formula  $d_L = |\Delta_{L/k}| d_k^2$  and the fact that  $d_k \leq V^{22}$  (proven as part of the proof of [58, Theorem 4.1]).  $\square$

We are now ready to prove Theorem 1.1. In what follows, let  $c_1, c_2$  be the constants appearing in Proposition 5.5,  $C$  be the constant appearing in Proposition 5.2 and  $c \geq C$  be such that  $c_1 e^{c_2 \log(V)V^7} \leq c e^{(\log(V)\log(V))}$  for all  $V \geq 0.9$ . (We note that the work of Chinburg, Friedman, Jones and Reid [20] implies that every arithmetic hyperbolic 3-manifold has volume  $V > 0.9427 \dots$ .)

*Proof of Theorem 1.1.* We will prove Theorem 1.1 in the case that the manifolds  $M_i$  are 3-manifolds and will then make a few remarks regarding the (minor) modifications needed for the 2-manifold case.

Let  $\Gamma_j$  be the fundamental groups of  $M_j$  for  $j = 1, 2$ . As in Reid's proof that isospectral arithmetic 3-manifolds are commensurable [84], it suffices to show that the quaternion algebras from which  $\Gamma_1$  and  $\Gamma_2$  arise are isomorphic. To that end, let  $(k_1, B_1)$  and  $(k_2, B_2)$  be the number fields and quaternion algebras giving rise to  $\Gamma_1$  and  $\Gamma_2$ .

By Proposition 5.2 there are hyperbolic elements  $\gamma_1 \in \Gamma_1$  and  $\gamma_2 \in \Gamma_2$  with non-real eigenvalues  $\lambda_{\gamma_1}$  and  $\lambda_{\gamma_2}$  whose associated closed geodesics have the same length. Taking powers of  $\gamma_1$  and  $\gamma_2$  if necessary, we may assume that  $\gamma_1 \in \Gamma_1^{(2)}$  and  $\gamma_2 \in \Gamma_2^{(2)}$ . It now follows that  $\text{tr}(\gamma_1)$  and  $\text{tr}(\gamma_2)$  differ by at most a sign [84, Lemma 1.4] and consequently that the images in  $\mathbf{C}$  of  $k_1$  and  $k_2$  coincide [21, Lemma 2.3]. We may therefore assume that  $B_1$  and  $B_2$  are defined over a common number field  $k$ .

We now show that  $B_1$  and  $B_2$  are isomorphic. Observe first that by Lemma 4.1 we have

$$|\text{disc}(B)|, |\text{disc}(B')| < 10^{57}V^7.$$

Suppose now that  $L$  is a quadratic extension of  $k$  which embeds into  $B_1$  and has norm of relative discriminant less than the bound given in Theorem 1.3; specifically, we employ the theorem with  $x = 10^{57}V^7$ . Proposition 5.5 then shows that there exists an element  $u_1 \in B$  such that  $L = k(u_1)$  with the property that the image  $\gamma_1$  of  $u_1$  in  $M(2, \mathbf{C})$  is a hyperbolic element lying in  $\Gamma_1$  and satisfies

$$\ell(\gamma_1) \leq c_1 e^{c_2 \log(V)V^7} \leq c e^{(\log(V)\log(V))}.$$

By hypothesis there is an element  $\gamma_2 \in \Gamma_2$  such that  $\ell(\gamma_1) = \ell(\gamma_2)$ . Let  $u_2$  be a preimage of  $\gamma_2$  in  $B_2$ . The formula for the length of the closed geodesics associated to  $\gamma_1, \gamma_2$  [84, Lemma 1.4] shows that (up to sign)  $\text{tr}(u_1) = \text{tr}(u_2)$ . Since the fields  $k(u_1)$  and  $k(u_2)$  are both isomorphic to  $L$ , we see that  $B_2$  admits an embedding of  $L$ . The same argument shows that if  $L'$  is a quadratic extension of  $k$  which embeds into  $B_2$  and has norm of relative discriminant less than the bound given in Theorem 1.3, again employed with  $x = 10^{57}V^7$ , then  $B_1$  admits an embedding of  $L'$ . Theorem 1.3 now shows that  $B_1 \cong B_2$ , finishing our proof.  $\square$

**Remark.** We briefly comment on the modifications needed for the 2-dimensional case of Theorem 1.1.

As was noted in the 3-dimensional case, it suffices to show that the quaternion algebras from which  $\Gamma_1$  and  $\Gamma_2$  arise are isomorphic. By Proposition 5.5 there exists an hyperbolic element  $\gamma \in \Gamma_1$  such that  $\ell(\gamma) \leq c_1 e^{c_2 \log(V)V^{130}}$ . Proposition 4.13 shows that we further have  $k_1 = \mathbf{Q}(\text{tr}(\gamma))$ .

By hypothesis there exists an element  $\gamma' \in \Gamma_2$  such that  $\ell(\gamma) = \ell(\gamma')$ , hence  $\text{tr}(\gamma) = \text{tr}(\gamma')$  (up to a sign). Since  $\mathbf{Q}(\text{tr}(\gamma)) = \mathbf{Q}(\text{tr}(\gamma'))$ , we may assume, as above, that  $k_1 = k_2$ .

The remainder of the proof is analogous to the proof of the 3-dimensional case. We simply note that in the 2-dimensional case we show that  $B_1 \cong B_2$  by showing that all maximal subfields of these algebras which have norm of relative discriminant less than the bound in Theorem 1.3 and are not totally complex coincide.

We conclude this section by proving the following strengthening of Theorem 1.1 in the case that the groups  $\Gamma_i$  are derived from orders in quaternion algebras.

**Theorem 5.6.** *Let  $k_1, k_2$  be totally real number fields (number fields which each contain a unique complex place, respectively) and  $B_1, B_2$  quaternion division algebras over  $k_1, k_2$  which are ramified at all but one real place (respectively, all real places) of  $k_1, k_2$ . Finally, let  $\mathcal{O}_1, \mathcal{O}_2$  be maximal orders in  $B_1, B_2$  and  $V$  be such that  $\text{covol}(\Gamma_{\mathcal{O}_1}), \text{covol}(\Gamma_{\mathcal{O}_2}) \leq V$ . There exist absolute effectively computable constants  $c_1, c_2, c_3$  such that if the length spectrum of  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}$  (respectively,  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}$ ) agrees with the length spectrum of  $\mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (respectively,  $\mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) for all lengths less than  $c_1 e^{c_2 \log(V)V^{130}}$  (respectively,  $c_3 e^{(\log(V)\log(V))}$ ) then  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (respectively,  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) are length-isospectral.*

*Proof.* Theorem 1.1 and its proof show that  $k_1 \cong k_2$  and  $B_1 \cong B_2$ , hence  $\mathcal{O}_2$  is isomorphic to a maximal order  $\mathcal{O} \subset B_1$ . If  $\mathcal{O} \cong \mathcal{O}_1$  then  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (or  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) will be isometric, hence isospectral and the theorem is clear. Suppose therefore that  $\mathcal{O} \not\cong \mathcal{O}_1$  and  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (or  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) are not isospectral. Theorem 3.3 of [19] and Theorem 12.4.5 of [65] now imply the existence of a quadratic extension  $L/k$  which is unramified at all finite places (and which is not totally complex if the

field  $k_1$  is totally real) and a quadratic order  $\Omega = \mathcal{O}_k[\gamma] \subset L$  such that  $\Omega$  embeds into exactly one of  $\{\mathcal{O}_1, \mathcal{O}\}$ . Proposition 4.7 indicates that there exist absolute constants  $C_1, C_2$  and a geodesic length

$$(24) \quad \ell(\gamma) \leq e^{C_1 V} d_k^{2C_2 + 2\log(V)} \leq e^{C_1 V} V^{44(C_2 + 2\log(V))},$$

which lies in the length spectrum of exactly one of  $\{\mathbf{H}^2/\Gamma_{\mathcal{O}}, \mathbf{H}^2/\Gamma_{\mathcal{O}_1}\}$  (or  $\{\mathbf{H}^3/\Gamma_{\mathcal{O}}, \mathbf{H}^3/\Gamma_{\mathcal{O}_1}\}$ ). We note that the latter inequality (24) follows from the proof of [58, Theorem 4.1]). By choosing constants appropriately we arrive at a contradiction to our hypothesis that the length spectra of  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (or  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) coincide for all sufficiently small lengths.  $\square$

## 6. GEOMETRIC SUBMANIFOLDS: EFFECTIVE RIGIDITY AND ASYMPTOTIC GROWTH OF SURFACES

We now turn our attention to an effective version of [70, Theorem 1.1] which stated that two arithmetic hyperbolic 3-manifolds with the same totally geodesic surfaces are commensurable provided they have a totally geodesic surface.

**6.1. Proof of Theorem 1.4.** Our first result is the algebraic version of this goal. Namely, we prove Theorem 1.4. Our proof will make use of the following easy extension of [65, Theorem 9.55] (whose proof will be omitted due to its similarity to the proof of [65, Theorem 9.55]).

**Theorem 6.1.** *Let  $L$  be a number field and let  $B$  be a quaternion algebra over  $L$  which is ramified precisely at the real places  $v_1, \dots, v_s$  of  $L$ . Let  $k$  be a subfield of  $L$  such that  $[L:k] = 2$  and  $B_0$  be a quaternion algebra over  $k$  which is ramified at  $v_1|_k, \dots, v_s|_k$  and at no other real places of  $k$ . Then  $B \cong B_0 \otimes_k L$  if and only if  $\text{Ram}_f(B)$  consists of the  $2r$  distinct places (with  $r$  possibly zero)*

$$\{\mathfrak{P}_1, \mathfrak{P}'_1, \dots, \mathfrak{P}_r, \mathfrak{P}'_r\},$$

where

$$\mathfrak{P}_i \cap \mathcal{O}_k = \mathfrak{P}'_i \cap \mathcal{O}_k = \mathfrak{p}_i$$

and  $\text{Ram}_f(B_0) \supset \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$  with  $\text{Ram}_f(B) \setminus \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$  consisting of primes in  $\mathcal{O}_k$  which are either ramified or inert in the extension  $L/k$ .

*Proof of Theorem 1.4.* Let  $R_1$  denote the set of places of  $L_1$  which ramify in  $B_1$ ,  $R_2$  denote the set of places of  $L_2$  which ramify in  $B_2$  and  $R'_i$  (for  $i = 1, 2$ ) denote the set of places of  $k$  lying below a place in  $R_i$ .

In light of our hypothesis that  $B_0 \otimes_k L_1 \cong B_1$  and  $B_0 \otimes_k L_2 \cong B_2$ , it suffices to show that  $L_1 \cong L_2$ . To that end, suppose that  $L_1 \not\cong L_2$  and let  $L$  be the compositum of  $L_1$  and  $L_2$ . Then the extension  $L/k$  is Galois with Galois group isomorphic to  $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ . Elementary properties of Frobenius elements [54, Chapter 10] show that if  $\mathfrak{p}_k$  is a prime of  $k$  which is unramified in  $L/k$  and whose Frobenius element  $(\mathfrak{p}_k, L/k)$  corresponds to the element  $(1, 1)$  of  $\text{Gal}(L/k)$  then  $\mathfrak{p}_k$  is inert in both  $L_1/k$  and  $L_2/k$ . Similarly, if the Frobenius element  $(\mathfrak{p}_k, L/k)$  corresponds to the element  $(1, 0)$  of  $\text{Gal}(L/k)$  then  $\mathfrak{p}_k$  is inert in  $L_1/k$  and splits in  $L_2/k$ . It now follows from the effective Chebotarev density theorem [53] (see also Theorem 5.3) that there exist primes  $\omega_1, \omega_2$  of  $k$  such that

- (i)  $\omega_1$  is inert in  $L_1/k$  and splits in  $L_2/k$ ,
- (ii)  $\omega_2$  is inert in both  $L_1/k$  and  $L_2/k$ ,
- (iii) Neither  $\omega_1$  nor  $\omega_2$  lie in  $R'_1 \cup R'_2$ ,

(iv)

$$|\omega_1|, |\omega_2| \leq d_k^C (2 \log(|\text{disc}(B_1)| |\text{disc}(B_2)|))^2.$$

Let  $B'$  be a quaternion algebra over  $k$  such that

$$\text{Ram}_\infty(B') = \{v|_k : v \in \text{Ram}_\infty(B_1)\}$$

and which ramifies at all primes lying in  $R'_1 \cup \{\omega_1\}$  (and possibly at  $\omega_2$  as well if needed for parity reasons). From our assumption about the existence of a  $k$ -algebra  $B_0$  such that  $B_0 \otimes_k L_1 \cong B_1$ , we deduce from Theorem 6.1 that  $B' \otimes_k L_1 \cong B_1$ . Recall that  $\omega_1$  splits in  $L_2/k$ . We can therefore write  $\omega_1 = v_1 v_2$  for primes  $v_1, v_2$  of  $k_2$ . Then  $(L_2)_{v_1} \cong k_{\omega_1}$ , which implies that

$$B_2 \otimes_{L_2} (L_2)_{v_1} \cong B' \otimes_k k_{\omega_1},$$

as by assumption we have  $B' \otimes_k L_2 \cong B_2$ . As  $\omega_1$  ramifies in  $B'$  we deduce that  $v_1$  ramifies in  $B_2$ , hence  $\omega_1 \in R'_2$ . This is a contradiction however, showing that  $L_1 \cong L_2$ .  $\square$

**6.2. Proof of Theorem 1.2.** We begin by recording a simple lemma about the coarea of certain arithmetic Fuchsian groups which will be needed to prove this section's main result.

**Lemma 6.2.** *Let  $B/k$  be a quaternion algebra and  $k$  a totally real field. If  $\mathcal{O}$  is a maximal order of  $B$ , then*

$$\text{coarea}(\Gamma_{\mathcal{O}}) \leq 2\pi^2 |\text{disc}(B)|.$$

*Proof.* Borel's volume formula [7] (see also [65, Chapter 11]) shows that

$$\text{coarea}(\Gamma_{\mathcal{O}}) = \frac{8\pi^2 \zeta_k(2) \prod_{\mathfrak{p}|\text{disc}(B)} (|\mathfrak{p}| - 1)}{(4\pi^2)^{n_k}}.$$

The inequality now follows from the well-known inequality  $\zeta_k(s) \leq \zeta(s)^{n_k}$ .  $\square$

**Proposition 6.3.** *Let  $M = \mathbf{H}^3/\Gamma$  be an arithmetic hyperbolic 3-manifold of volume  $V$  with invariant quaternion algebra  $B$  and trace field  $L$ . Suppose that  $k = L^+$  is the maximal totally real subfield of  $L$  and that  $[L : k] = 2$ . Let  $B_0$  be a quaternion algebra over  $k$  such that  $B_0 \otimes_k L \cong B$ . Then there exists an absolute effectively computable constant  $C$  such that  $M$  contains a totally geodesic surface with area at most  $2\pi^2 |\text{disc}(B_0)| e^{CV}$ .*

*Proof.* Let  $\mathcal{O}_0$  be a maximal order of  $B_0$  and  $\mathcal{O}$  a maximal order of  $B$  such that  $\Gamma_{\mathcal{O}_0} \subset \Gamma_{\mathcal{O}}$ . Let  $\Gamma^{(2)}$  be the subgroup of  $\Gamma$  generated by squares and define

$$\Delta = \Gamma_{\mathcal{O}_0} \cap \Gamma^{(2)}.$$

Then  $\Delta$  is a Fuchsian group contained in  $\Gamma$  and we have

$$[\Gamma_{\mathcal{O}_0} : \Delta] \leq [\Gamma : \Gamma^{(2)}].$$

By Lemma 4.3,

$$[\Gamma : \Gamma^{(2)}] \leq e^{CV},$$

where  $C$  is an absolute effectively computable constant. The Proposition now follows from Lemma 6.2.  $\square$

For a hyperbolic 3-manifold  $M$ , we denote by  $GS(M)$  the collection of isometry types of totally geodesic surfaces. We can prove our main result of this section, an effective version of [70, Theorem 1.1].

*Proof of Theorem 1.2.* Let  $M_1 = \mathbf{H}^3/\Gamma_1$ ,  $M_2 = \mathbf{H}^3/\Gamma_2$  and  $B_1/L_1, B_2/L_2$  be the invariant quaternion algebras and trace fields of  $M_1$  and  $M_2$ . Since  $GS(M_1) \neq \emptyset$ ,  $\Gamma_1$  contains a non-elementary Fuchsian group. By considering the invariant quaternion algebra and trace field of this Fuchsian group we see that the maximal totally real subfield  $k$  of  $L_1$  satisfies  $[L_1 : k] = 2$ . As  $GS(M_1) \cap GS(M_2)$  is non-empty, we see that  $[L_2 : k] = 2$  and also that there exists a quaternion algebra  $B_0$  over  $k$  such that  $B_0 \otimes_k L_1 \cong B_1$  and  $B_0 \otimes_k L_2 \cong B_2$ .

Let  $C$  be the constant appearing in the effective Chebotarev density theorem [53] (see also Theorem 5.3). By combining the estimates  $d_k \leq d_{L_1} \leq V^{22}$  (proven as a part of [58, Theorem 4.1]) and

$$|\text{disc}(B_1)|, |\text{disc}(B_2)| \leq 10^{57} V^7$$

(proven in Lemma 4.1), we see that elementary computations show the existence of an absolute constant  $C_1$  such that

$$V^{C_1} \geq d_k^{2C} (2 \log(|\text{disc}(B_1)| |\text{disc}(B_2)|))^4 |\text{disc}(B_1)| |\text{disc}(B_2)|.$$

Let  $C_2$  be the constant appearing in Proposition 6.3 and choose  $C_3$  so that

$$2\pi^2 V^{C_1} e^{C_2 V} \leq e^{C_3 V}.$$

Note that our constant  $C_3$  may be chosen independently of  $M_1, M_2$  and  $V$ .

We will now show that if a finite type hyperbolic surface  $X$  lies in  $GS(M_1)$  if and only it lies in  $GS(M_2)$  whenever the area of  $X$  is less than  $e^{C_3 V}$ , then  $M_1$  and  $M_2$  are commensurable.

Let  $B'$  be a quaternion algebra over  $k$  which is ramified at all real places of  $k$  except the identity and satisfies

$$|\text{disc}(B')| \leq d_k^{2C} (2 \log(|\text{disc}(B_1)| |\text{disc}(B_2)|))^4 |\text{disc}(B_1)| |\text{disc}(B_2)|$$

as well as  $B' \otimes_k L_1 \cong B_1$ . Proposition 6.3 and the discussion above show that  $M_1$  contains a totally geodesic surface  $X$  (arising from the quaternion algebra  $B$ ) with area at most  $e^{C_3 V}$ . Our assumption therefore implies that  $M_2$  contains a totally geodesic surface isometric to  $X$  as well. Consequently we see that we must have  $B' \otimes_k L_2 \cong B_2$ . Interchanging the roles of  $B_1$  and  $B_2$  we see that by Theorem 1.4,  $L_1 \cong L_2$  and  $B_1 \cong B_2$ . Theorem 8.4.1 of [65] shows that this means that  $M_1$  and  $M_2$  are commensurable.  $\square$

**6.3. Proof of Theorem 1.11.** We conclude this section with a proof of Theorem 1.11.

*Proof of Theorem 1.11.* Let  $k = L^+$  denote the maximal totally real subfield of  $L$ . The hypothesis that  $M$  contains a totally geodesic surface implies that  $[L : k] = 2$ . Theorem 2.7, along with a slight modification to the proof of Theorem 1.7 in the case that  $r = 1$ , shows that there exists a constant  $c(L)$  depending only on  $L$  (actually the constant depends only on  $k$ ) such that for sufficiently large  $x$  the number of quaternion algebras  $B'$  over  $k$  satisfying  $B' \otimes_k L \cong B$  and  $|\text{disc}(B')| \leq x$  is asymptotic to

$$\left[ c(L) \text{disc}(B)^{1/2} \right] x / \log(x)^{1/2}.$$

The theorem now follows from Proposition 6.3.  $\square$

**Remark.** An immediate consequence of Theorem 1.11 is the well-known fact that if an arithmetic hyperbolic 3-manifold contains a totally geodesic surface then it in fact contains infinitely many.

## 7. LIMITATIONS AND EXTREMES

Throughout this paper, on the geometric side we have been able to prove a number of results of a certain flavor. Namely, given a fixed arithmetic manifold  $M$  with some volume upper bound  $V$  and a geometric invariant indexed with respect to some complexity (length, volume), we can determine the commensurability class by going (explicitly) far enough out in our set of invariants. In this section, we produce examples that test the limits of that work.

**7.1. Tower construction.** In this subsection, we give a covering construction that shows that incommensurable arithmetic hyperbolic 3-manifolds can share arbitrarily large portions of their primitive geodesic length set.

We start with a pair of incommensurable, arithmetic hyperbolic 3-manifolds  $M_1, M_2$  that both have a common totally geodesic surface  $N$ . There are a number of ways to produce these manifolds. For instance, take a totally real field  $k$  with a quaternion algebra  $B_0$  that is ramified at precisely one real place. Next, we select quadratic extensions  $L_1, L_2$  of  $k$  that have exactly one complex place and such that  $B_j = B_0 \otimes_k L_j$  is ramified at every real place of  $L_j$ . We then take a maximal order  $\mathcal{O}_0$  in  $B_0$  and maximal orders  $\mathcal{O}_j$  in  $B_j$  with  $\mathcal{O}_0 \subset \mathcal{O}_j$ . Finally, we take torsion free, finite index subgroups  $\Gamma_j < \Gamma_{\mathcal{O}_j}$  such that

$$\Delta = \Gamma_{\mathcal{O}_0} \cap \Gamma_1 = \Gamma_{\mathcal{O}_0} \cap \Gamma_2.$$

The manifolds  $M_1, M_2$  can be selected so that  $\pi_1(N) < \pi_1(M_j)$  is subgroup separable by which we mean that

$$\bigcap_{\substack{\Lambda < \pi_1(M_j), \\ [\pi_1(M_j):\Lambda] < \infty, \\ \pi_1(N) < \Lambda}} \Lambda = \pi_1(N).$$

We can arrange the separability either with some additional care in our selections or by employing the recent works of Agol and Wise (see for instance [1]) to ensure it. The infinite volume manifold  $\mathbf{H}^3/\pi_1(N)$  has for its set of primitive geodesic lengths those that are primitive geodesic lengths on the surface  $N$ . Set  $L_p(N)$  to be the set of (primitive) geodesic lengths on the surface  $N$  ordered by size. As  $\pi_1(N)$  is separable, we have a tower of finite covers  $M_{j,k}$  such that

$$\bigcap_{k=1}^{\infty} L_p(M_{j,k}) = L_p(N).$$

Of course,

$$L_p(M_{j,1}) \supseteq L_p(M_{j,2}) \supseteq L_p(M_{j,3}) \supseteq \cdots \supseteq L_p(N).$$

In particular, we can arrange the tower so that the first  $r$  primitive lengths on  $N$  are precisely the first  $r$  lengths on  $L_p(M_{j,r})$ .

A simple example of a pair of arithmetic hyperbolic 3-orbifolds with a common, separable, totally geodesic surface is given by the orbifold fundamental groups  $\mathrm{PSL}(2, \mathcal{O}_{L_1}), \mathrm{PSL}(2, \mathcal{O}_{L_2})$ , where  $L_1, L_2$  are distinct imaginary quadratic number fields. The surface fundamental group can be taken to be the modular group  $\mathrm{PSL}(2, \mathbf{Z})$ . In this particular example, the separation of the subgroup  $\mathrm{PSL}(2, \mathbf{Z})$  is rather easy and provides bounds on the indices of the subgroups in  $\mathrm{PSL}(2, \mathcal{O}_{L_1})$  and  $\mathrm{PSL}(2, \mathcal{O}_{L_2})$  used in the above covering construction. Ordering the split primes  $\mathcal{P}_s(L_j)$  in  $\mathcal{O}_{L_j}$  by their norms, we have reduction homomorphisms

$$r_{\mathfrak{p}}: \mathrm{PSL}(2, \mathcal{O}) \longrightarrow \mathrm{PSL}(2, \mathcal{O}/\mathfrak{p}) \cong \mathrm{PSL}(2, \mathbf{F}_{p^2})$$



given by reducing the coefficients of the matrices modulo  $\mathfrak{p}$ . The image of  $\mathrm{PSL}(2, \mathbf{Z})$  will be in the smaller finite subgroup  $\mathrm{PSL}(2, \mathbf{F}_p)$ . For any element  $\gamma \in \mathrm{PSL}(2, \mathcal{O}_{L_j}) - \mathrm{PSL}(2, \mathbf{Z})$ , one simply takes the smallest prime in  $\mathcal{P}_s(L_j)$  where a coefficient of  $\gamma$  modulo this prime is not in the prime field  $\mathbf{F}_p$ . This can be done quite efficiently as a function of the complexity of  $\gamma$  (either in terms of geodesic length or word length). In terms of word length, the norm of the prime can be taken to be roughly the length of the word and so the index of the subgroup that contains  $\mathrm{PSL}(2, \mathbf{Z})$  but not  $\gamma$  is

$$[\mathrm{PSL}(2, \mathbf{F}_{p^2}) : \mathrm{PSL}(2, \mathbf{F}_p)] \approx p^3 \approx |\gamma|^3,$$

where  $|\gamma|$  denotes the word length in a fixed but unspecified finite generating set for  $\mathrm{PSL}(2, \mathcal{O}_{L_j})$ . Explicitly, the subgroup  $\Lambda_{\gamma,j} < \mathrm{PSL}(2, \mathcal{O}_{L_j})$  is

$$\Lambda_{\gamma,j} = r_{\mathfrak{p}}^{-1}(\mathrm{PSL}(2, \mathbf{F}_p)).$$

**Remark.** Ensuring that  $\gamma$  has non-trivial image in some finite quotient cannot be done in quotient groups smaller than  $|\gamma|^{2/3}$  in general (see [10] or [50]). Here, we are asking more in that we also want our element  $\gamma$  to have an image outside the image of the subgroup  $\mathrm{PSL}(2, \mathbf{Z})$ . Our argument above, which achieves this stronger demand, separates with subgroups of index no worse than  $|\gamma|^3$ . In particular, our covering construction for this example is close to optimal with regard to the minimizing the degrees of the covers. One can get an explicit upper bound for the volumes of the covers used to match the first  $n$  geodesic lengths from these degrees.

**7.2. Limits of the recovering of commensurability classes from surfaces.** In this subsection, we give a construction of a pair of incommensurable, arithmetic hyperbolic 3-manifolds with the same set of commensurability classes of surfaces up to an arbitrary threshold. We will provide a purely algebraic construction and trust that the reader can translate the construction to the geometric side via Theorem 2.7. Our goal is to construct a pair of quaternion algebras  $B_1, B_2$  over number fields  $L_1, L_2$  with exactly one complex place and a totally real subfield  $k$  with  $[L_j : k] = 2$  such that if  $B/k$  is a quaternion algebra over  $k$  with discriminant bounded by some  $x$ , then  $B_1 \cong B \otimes_k L_1$  if and only if  $B_2 \cong B \otimes_k L_2$ . Constructions of this type were implemented in [69] where this held for all algebras  $B$ . However, in [69], the fields  $L_j$  needed to be locally equivalent (same ring of adèles) and thus cannot share a common quadratic subfield.

Assume that we have two imaginary quadratic fields  $L_1, L_2$  such that all the integer primes have the same splitting behavior in  $L_1, L_2$  up to some integer  $m$ . We take two quaternion algebras  $B_1, B_2$  defined over  $L_1, L_2$  that have the same local invariants at the primes above these integer primes up to  $m$ . We can arrange it so that there is an algebra  $B/\mathbf{Q}$  such that

$$B_1 \cong B \otimes_{\mathbf{Q}} L_1, \quad B_2 \cong B \otimes_{\mathbf{Q}} L_2.$$

By construction,  $B_1, B_2$  will share the same algebras  $B$  with this property and the additional condition that  $B$  is unramified at every prime larger than  $m$ . As  $L_1, L_2$  are distinct, there must be a pair of primes  $p_1, p_2$  that split in  $L_1$  but are inert in  $L_2$ . We may furthermore arrange it so that  $B_2$  is ramified at these primes while  $B_1$  is unramified at them. We see that if  $B$  tensors up to either  $B_1, B_2$ , we must have  $B$  ramified in one case while in the other case  $B$  can be ramified or unramified. This produces an algebra that resides in one but not the other despite the fact that the two algebras have the same subalgebras coming from  $\mathbf{Q}$  up to a certain discriminant. This construction allows us to produce distinct algebras with arbitrarily large overlaps on subalgebras coming from  $\mathbf{Q}$ .



In [70], examples of manifolds with precisely the same set of totally geodesic surfaces were produced using the broad philosophy employed for producing arithmetically equivalent number fields via Gassmann equivalent subgroups of a finite group. As with the method of Sunada, the examples are necessarily commensurable.

## 8. EIGENVALUES

It is well-known that the Selberg trace formula equates the eigenvalue spectrum of the Laplace–Beltrami operator and the primitive geodesic length spectrum of a hyperbolic 2– or 3–manifold. Consequently, two Riemann surfaces  $X, Y$  of genus  $g$  have the same eigenvalue spectrum if and only if they have the same primitive geodesic length spectrum. Buser–Courtois [15] proved an effective result for both spectra for Riemann surfaces. Namely, they proved the following theorem.

**Theorem 8.1** (Buser–Courtois). *There exists an integer  $m = m(g, \varepsilon)$  with the following property. If  $X, Y$  are Riemann surfaces of genus  $g$  with injectivity radius bounded below by  $\varepsilon$  and have the same first  $m$  eigenvalues then all the eigenvalues are the same.*

As we mentioned above, Buser–Courtois also established this result for geodesic lengths. From this result and the ideas used within the proof of Theorem 5.6, one should be able to work out an explicit bound for  $m(g, \varepsilon)$ . Kelmer has two recent and related results. First, Kelmer [51] shows that if two compact, hyperbolic  $n$ –manifolds have the same multiplicities, up to some small error, then the two manifolds must be isospectral. Second, Kelmer [52] proves that if two non-compact, finite volume, even dimensional hyperbolic manifolds have the same geodesic lengths, up to a finite error, the two manifolds must be isospectral.

In order to transfer our effective rigidity results for geodesic lengths to effective rigidity results for eigenvalues on hyperbolic surfaces, we need to know that given an integer  $m$ , there exists an integer  $n_m$  such that for a Riemann surface  $X$ , the first  $m$  eigenvalues for the Laplace–Beltrami operator on  $X$  are determined by the first  $n_m$  geodesic lengths on  $X$ . We do not know if such a result is known. Moreover, since we seek effectively computable constants, the size of  $n_m$  would need to be explicitly bounded as a function of  $m$ . We could ask for slightly less and allow  $n$  to depend on both  $X$  and  $m$ . Since we are working with arithmetic surfaces, there are only finitely many possibilities for  $X$  for a fixed compact surface as the underlying space. In particular, allowing  $X$  to vary in our setting adds very little.

In higher dimensions, Colin de Verdière [26] proved that for any finite set

$$\{\alpha_0 \leq \alpha_1 \leq \cdots \leq \alpha_n\} \subset [0, \infty)$$

and any smooth, closed  $n$ –manifold  $M$ , there exists a Riemannian metric  $g$  on  $M$  with  $\lambda_j(M, g) = \alpha_j$ . In particular, in the general space of metrics, effective rigidity results are likely impossible.

## REFERENCES

- [1] I. Agol, *The virtual Haken conjecture*, with an appendix by Agol, Daniel Groves, and Jason Manning. Doc. Math. **18** (2013), 1045–1087.
- [2] J. Athreya, A. Bufetov, A. Eskin, and M. Mirzakhani, *Lattice point asymptotics and volume growth on Teichmüller space*, Duke Math. J. **161** (2012), 1055–1111.
- [3] M. Belolipetsky, *Counting maximal arithmetic subgroups*, with an appendix by Jordan Ellenberg and Akshay Venkatesh. Duke Math. J. **140** (2007), 1–33.

- [4] M. Belolipetsky, T. Gelander, A. Lubotzky, and A. Shalev, *Counting arithmetic lattices and surfaces*, Ann. of Math. (2) **172** (2010), 2197–2221.
- [5] M. Belolipetsky and A. Lubotzky, *Manifolds counting and class field towers*, Adv. Math. **229** (2012), 3123–3146.
- [6] M. Bhargava. Higher composition laws and applications. In *International Congress of Mathematicians. Vol. II*, pages 271–294. Eur. Math. Soc., Zürich, 2006.
- [7] A. Borel, *Commensurability classes and volumes of hyperbolic 3-manifolds*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **8**(1) (1981), 1–33.
- [8] A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. (2) **75** (1962) 485–535.
- [9] A. Borel and G. Prasad, *Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups*, Inst. Hautes Études Sci. Publ. Math., **69** (1989) 119–171.
- [10] K. Bou-Rabee and D. B. McReynolds, *Asymptotic growth and least common multiples in groups*, Bull. Lond. Math. Soc. **43** (2011), 1059–1068.
- [11] B. Brindza, *On the generators of  $S$ -unit groups in algebraic number fields*, Bull. Austral. Math. Soc., **43** (1991), 325–329.
- [12] S. Brueggeman and D. Doud, *Local corrections of discriminant bounds and small degree extensions of quadratic base fields*, Int. J. Number Theory, **4** (2008), 349–361.
- [13] M. Burger, T. Gelander, A. Lubotzky, and S. Mozes, *Counting hyperbolic manifolds*, Geom. Funct. Anal. **12** (2002), 1161–1173.
- [14] P. Buser, *Geometry and spectra of compact Riemann surfaces*, Modern Birkhäuser Classics. Birkhäuser Boston, 2010.
- [15] P. Buser and G. Courtois, *Finite parts of the spectrum of a Riemann surface*, Math. Ann. **287** (1990), 523–530.
- [16] J. W. S. Cassels and A. Frölich, *Algebraic number theory*, London Mathematical Society, 1967.
- [17] V. I. Chernousov, A. S. Rapinchuk, and I. A. Rapinchuk, *On the genus of a division algebra*, C. R. Math. Acad. Sci. Paris **350** (2012), 17–18.
- [18] T. Chinburg and E. Friedman, *The smallest arithmetic hyperbolic three-orbifold*, Invent. Math., **86** (1986), 507–527.
- [19] T. Chinburg and E. Friedman, *An embedding theorem for quaternion algebras*, J. London Math. Soc. (2) **60** (1999), 33–44.
- [20] T. Chinburg, E. Friedman, K. N. Jones, and A. W. Reid, *The arithmetic hyperbolic 3-manifold of smallest volume*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4), **30** (2001), 1–40.
- [21] T. Chinburg, E. Hamilton, D. D. Long, and A. W. Reid, *Geodesics and commensurability classes of arithmetic hyperbolic 3-manifolds*, Duke Math. J., **145** (2008), 25–44.
- [22] T. Chinburg and A. W. Reid, *Closed hyperbolic 3-manifolds whose closed geodesics all are simple*, J. Diff. Geom. **38** (1993), 545–558.
- [23] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Enumerating quartic dihedral extensions of  $\mathbf{Q}$* , Compos., **133** (2002), 65–93.
- [24] H. Cohen, *Constructing and counting number fields*, In Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), p. 129–138, 2002. Higher Ed. Press.
- [25] H. Cohn, *The density of abelian cubic fields*, Proc. Amer. Math. Soc. **5** (1954), 476–477.
- [26] Y. Colin de Verdière, *Construction de laplaciens dont une partie finie du spectre est donnée*, Annales scientifiques de l’École Normale Supérieure, Sér. 4, **20** (1987), 599–615.
- [27] B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math., **386** (1988), 116–138.
- [28] H. Davenport and H. Heilbronn. *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A, **322** (1971), 405–420.
- [29] H. Delange, *Théorèmes taubériens et applications arithmétiques*, Mém. Soc. Roy. Sci. Liège (4) **16** (1955), no. 1–2, 87 pp.
- [30] H. Delange, *Généralisation du théorème de Ikehara*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 213–242.
- [31] W. Duke, Z. Rudnick and P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke Math. J. **71** (1993), 143–179.
- [32] P. Dusart, *Estimates of some functions over primes without  $R. H.$* , <http://arxiv.org/abs/1002.0442>.
- [33] A. Eskin and C. McMullen, *Mixing, counting, and equidistribution in Lie groups*, Duke Math. J. **71** (1993), 181–209.
- [34] A. Eskin and M. Mirzakhani, *Counting closed geodesics in moduli space*, J. Mod. Dyn. **5** (2011), 71–105.
- [35] A. Eskin, S. Mozes and N. Shah, *Unipotent flows and counting lattice points on homogeneous varieties*, Ann. Math. (2) **143** (1996), 253–299.
- [36] R. Gangolli, *The length spectra of some compact manifolds*, J. Diff. Geom. **12** (1977), 403–424.
- [37] S. Garibaldi and D. Saltman, *Quaternion algebras with the same subfields*, Quadratic forms, linear algebraic groups, and cohomology: Developments in Mathematics, **18** Springer, (2010), 225–238.
- [38] T. Gelander, *Homotopy type and volume of locally symmetric manifolds*, Duke Math. J. **124** (2004), 459–515.
- [39] T. Gelander, *Volume versus rank of lattices*, J. Reine Angew. Math. **661** (2011), 237–248

- [40] T. Gelander and Y. Glasner, *Countable primitive groups*, *Geom. Funct. Anal.* **17** (2008), 1479–1523.
- [41] T. Gelander and A. Levit, *Counting commensurability classes of hyperbolic manifolds*, <http://front.math.ucdavis.edu/1401.8003>, to appear in *Geom. Funct. Anal.*
- [42] R. Godement, *Domaines fondamentaux des groupes arithmétiques*, Séminaire Bourbaki, 1962/63. Fasc. 3, No. 257 25 pp. Secrétariat mathématique, Paris.
- [43] D. Goldfeld, A. Lubotzky, N. Nikolov, and L. Pyber, *Counting primes, groups, and manifolds*, *Proc. Natl. Acad. Sci. USA* **101** (2004), 13428–13430.
- [44] D. Goldfeld, A. Lubotzky, and L. Pyber, *Counting congruence subgroups*, *Acta Math.* **193** (2004), 73–104.
- [45] A. S. Gelfsfidy, *Counting lattices in simple Lie groups: the positive characteristic case*, *Duke Math. J.* **161** (2012), 431–481.
- [46] C. S. Gordon, *Survey of isospectral manifolds*, *Handbook of differential geometry*, Vol. I, 2000, 747–778.
- [47] A. Gorodnik and H. Oh, *Rational points on homogeneous varieties and equidistribution of adelic periods*, with an appendix by Mikhail Borovoi. *Geom. Funct. Anal.* **21** (2011), 319–392.
- [48] L. Hajdu, *A quantitative version of Dirichlet’s  $S$ -unit theorem in algebraic number fields*, *Publ. Math. Debrecen*, **42** (1993), 239–246.
- [49] H. Huber, *Zur analytischen theorie hyperbolischer Raumformen und Bewegungsgruppen. II*, *Math. Ann.* **143** (1961), 463–464.
- [50] M. Kassabov and F. Matucci, *Bounding the residual finiteness of free groups* *Proc. Amer. Math. Soc.* **139** (2011), 2281–2286.
- [51] D. Kelmer, *A refinement of strong multiplicity one for spectra of hyperbolic manifolds*, <http://front.math.ucdavis.edu/1108.2977>, to appear in *Tran. Amer. Soc.*
- [52] D. Kelmer, *On distribution of poles of Eisenstein series and the length spectrum of hyperbolic manifolds*, <http://front.math.ucdavis.edu/1402.4780>.
- [53] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, *Invent. Math.*, **54**(1979), 271–296.
- [54] S. Lang, *Algebraic number theory*, Springer-Verlag, 1994.
- [55] M. Larsen and A. Lubotzky, *Representation growth of linear groups*, *J. Eur. Math. Soc.* **10** (2008), 351–390.
- [56] M. Liebeck and A. Shalev, *Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks*, *J. Algebra* **276** (2004), 552–601.
- [57] B. Linowitz, *Selectivity in quaternion algebras*, *J. of Number Theory*, **132** (2012), 1425–1437.
- [58] B. Linowitz, *Families of mutually isospectral Riemannian orbifolds*, <http://arxiv.org/abs/1309.0499>
- [59] S. Louboutin, *The Brauer–Siegel theorem*, *J. London Math. Soc.* (2), **72** (2005), 40–52.
- [60] A. Lubotzky and N. Nikolov, *Subgroup growth of lattices in semisimple Lie groups*, *Acta Math.* **193** (2004), 105–139.
- [61] A. Lubotzky, B. Samuels, and U. Vishne, *Division Algebras and Non-Commensurable Isospectral Manifolds*, *Duke Math. J.* **135** (2006), 361–379.
- [62] A. Lubotzky and D. Segal, *Subgroup growth*, *Progress in Mathematics*, **212**, Birkhäuser Verlag, 2003.
- [63] A. Macbeath, *Commensurability of cocompact three dimensional hyperbolic groups*, *Duke Math. J.* **50** (1983), 1245–1253.
- [64] C. Maclachlan and A. W. Reid, *Commensurability classes of arithmetic Kleinian groups and their Fuchsian subgroups*, *Math. Proc. Cambridge Philos. Soc.* **102** (1987), 251–257.
- [65] C. Maclachlan and A. W. Reid, *The Arithmetic of Hyperbolic 3–Manifolds*, *Grad. Texts in Math.* **219**, Springer (2003).
- [66] D. A. Marcus, *Number fields*, Springer-Verlag, 1977.
- [67] G. A. Margulis, *Certain applications of ergodic theory to the investigation of manifolds of negative curvature*, *Funkcional. Anal. i Prilozhen.* **3** (1969), 89–90.
- [68] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, Springer-Verlag, 1991.
- [69] D. B. McReynolds, *Geometric spectra and commensurability*, <http://front.math.ucdavis.edu/1401.1516>, to appear in *Cand. Jour. Math.*
- [70] D. B. McReynolds and A. W. Reid, *The genus spectrum of a hyperbolic 3–manifold*, <http://front.math.ucdavis.edu/0901.4086>, to appear in *Math. Res. Lett.*
- [71] J. Meyer, *Division algebras with infinite genus*, <http://arxiv.org/abs/1301.5632>.
- [72] C. Millichap, *Factorial growth rates for the number of hyperbolic 3-manifolds of a given volume* to appear in *PAMS* <http://arxiv.org/abs/1209.1042>
- [73] C. Millichap, *Mutations and short geodesics in hyperbolic 3-manifolds*, <http://front.math.ucdavis.edu/1406.6033>.
- [74] M. Mirzakhani, *Growth of the number of simple closed geodesics on hyperbolic surfaces*, *Ann. of Math.* (2) **168** (2008), 97–125.
- [75] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, *Sém. Théor. Nombres Bordeaux* (2) **2** (1990), 119–141.

- [76] R. S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, **88**. Springer–Verlag, 1982.
- [77] A. Pethő and S. Schmitt, *Elements with bounded height in number fields*, Period. Math. Hungar., **43** (2001), 31–41.
- [78] V. Platonov and A. Rapinchuk, *Algebraic groups and number fields*, Academic Press, 1994.
- [79] G. Poitou, *Sur les petits discriminants*, In *Séminaire Delange–Pisot–Poitou, 18e année: (1976/77), Théorie des nombres, Fasc. 1 (French)*, pages Exp. No. 6, 18. Secrétariat Math., Paris, 1977.
- [80] G. Prasad and A. Rapinchuk, *Weakly commensurable arithmetic groups and isospectral locally symmetric spaces*, Publ. Math., Inst. Hautes Étud. Sci. **109** (2009), 113–184.
- [81] J. Raimbault, *A note on maximal lattice growth in  $SO(1, n)$* , Int. Math. Res. Not. **16** (2013), 3722–3731.
- [82] M. S. Raghunathan, *Discrete subgroups of Lie groups*, Springer–Verlag, 1972.
- [83] A. W. Reid, *A note on trace fields of Kleinian groups*, Bull. London Math. Soc. **22** (1990), 349–352.
- [84] A. W. Reid, *Isospectrality and commensurability of arithmetic hyperbolic 2- and 3-manifolds*, Duke Math. J., **65** (1992), 215–228.
- [85] I. Reiner, *Maximal orders*, London Mathematical Society Monographs, **28**. Oxford University Press, 2003.
- [86] I. Rivin, *Simple curves on surfaces*, Geom. Dedicata **87** (2001), 345–360.
- [87] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math., **54** (1981), 323–401.
- [88] T. Sunada, *Riemannian coverings and isospectral manifolds*, Ann. of Math. (2) **121** (1985), 169–186.
- [89] K. Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **24** (1977), 201–212.
- [90] J. Tits, *Classification of algebraic semisimple groups*, Algebraic Groups and Discontinuous Subgroups, Amer. Math. Soc. (1966), 33–62.
- [91] W. P. Thurston, *The Geometry and Topology of 3-manifolds*, Princeton University, mimeographed notes (1979).
- [92] M.-F. Vignéras, *Variétés riemanniennes isospectrales et non isométriques*, Ann. of Math. (2) **112** (1980), 21–32.
- [93] S. Wang, *An effective version of the Grunwald–Wang theorem*, Ph.D. thesis, Caltech, 2001.
- [94] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Annalen, **143** (1961), 75–102.
- [95] M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math., **146** (2010), 102–128.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109

*E-mail address:* linowitz@umich.edu

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, WEST LAFAYETTE, IN 47907

*E-mail address:* dmcreyno@purdue.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602

*E-mail address:* pollack@uga.edu

DEPARTMENT OF MATHEMATICS, OBERLIN COLLEGE, OBERLIN, OH 44074

*E-mail address:* lola.thompson@oberlin.edu